CHAKTIN_YU_GCFW.PDF

SANS GCFW PRACTICAL ASSIGNMENT

Yu Chak Tin

michael242

GCFW

Version 1.7

Original submission

Challenge

Table of Contents

Assignment 1

Define a security architecture for GIAC Enterprise, an e-business which conducts online sale of fortune cookie sayings.

Introduction

A security architecture enforces an organization's security policies. To develop a truly effective security solution, the policies must first be clearly defined. For this project, the security policies are introduced in Assignment 2 – Part -1.

Business Requirement

The design of the GIAC security architecture has to satisfy the requirements listed below:

■   External customers are buying goods and making payments online securely.
■   External partners and suppliers are accessing and updating the ecommerce resource database securely. BOTH the external partners and the suppliers collaborate with GIAC via the use of the GIAC critical database application. This application provides a standardized web based interface, and each partner / supplier is assigned a set of unique login profile and privileges.
■   Company staffs occasionally need to access in-house server resources from home.
■   Internal staffs frequently need to access the internet.
■   GIAC is experiencing tremendous business growth these days.

Technical Requirement

We need to translate GIAC's business requirements into a set of technical requirements. These requirements are defined based on the four major traffic streams: B2C, B2B, INET and RAS.
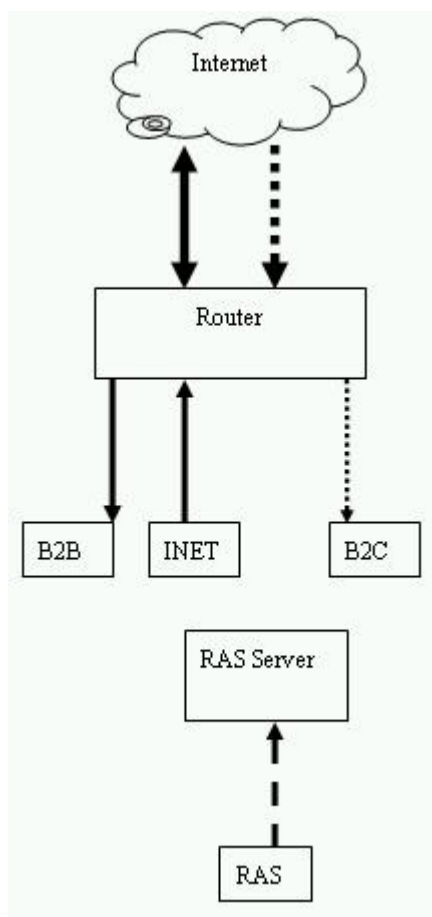
For performance reason, a minimum of two internet links are deployed, with one devoted to servicing the customers (B2C) and the other one for servicing access requests from external partners and suppliers (B2B) as well as outgoing internet requests made by the internal staffs (INET). RAS access (RAS) is made available via direct dial in, and has nothing to do with the internet.

B2C:

* This is the link with the highest exposure to security threats.

B2C traffic includes inbound requests for the following services:
- ◊   Ecommerce web service – TCP port 80 (HTTP) and 443 (SSL)
- ◊   External email service – TCP port 25 (SMTP)
- ◊   External DNS service – UDP port 53 (DNS request)

❑ SSL and digital certificates are deployed by the ecommerce web site. Such capabilities are built-in to the web server.

❑ Two sets of DNS systems are in place, one for external use and one for internal use. This is known as "DNS Split Horizon".

❑ Two sets of SMTP messaging systems are in place, one for external use and one for internal use.

❑ All servers are Microsoft Windows based.

❑ The Ecommerce web application is updated by the internal web developers via standard protocol (HTTP / HTTPS) based method, such as FrontPage Server extension. Microsoft Networking is not involved in the update activities.

B2B:

B2B is about the secure communication process between GIAC and its external partners & suppliers. Since the communication medium is the internet, VPN technology is used. The database application server allows access via a standard HTTP/HTTPS interface for ease of control and administration.

Regarding the VPN model, a router-to-router VPN model is not deployed primarily because the volume of use between the partnering organizations does not justify a fixed router-to-router setup. Instead, a Remote Access PPP based VPN solution is deployed to give flexibility and simpler configuration. For this reason, incoming VPN traffic is to be processed by a VPN server while outgoing traffic is not (outgoing VPN connections to external partners are configured on the client side for users who need such access. No server side setting is involved in GIAC network for outbound VPN requests).

B2B traffic includes requests for the following:

◊ Remote access via VPN from the external partners and suppliers to the database application server. For security and ease of control / administration, a standardized web based interface is used. For this to work, TCP port 80 must be used.

INET:

INET traffic accommodates outbound requests for the following:

◊ Internal staffs accessing the internet: HTTP, HTTPS, FTP, SMTP

◊ Internal staffs as VPN clients accessing external partners' secure sites via PPTP

RAS:

Company staffs are accessing the in-house server resources from home or from business trips via RAS dial-in. RAS traffic does not pass through the router.

Architecture Overview

A firewall is a system designed to prevent unauthorized access to or from a private network. It can be implemented in both hardware and software, or a combination of both. Since all messages entering or leaving the internal network must pass through the firewall for security examination, the firewall itself is a potential bottleneck. Also, regardless of how a firewall is implemented, a good firewall product costs a large sum of money.

Our goal for the security architecture of GIAC Enterprise is to secure its network and at the same time achieve a balance between security, performance and cost. To achieve such balance, at the front line we use higher end security products, while at the departmental level we use more economical solutions.

Design Principle and Tradeoff

The exhibit below shows that multiple firewall and routing devices are deployed in the architecture.
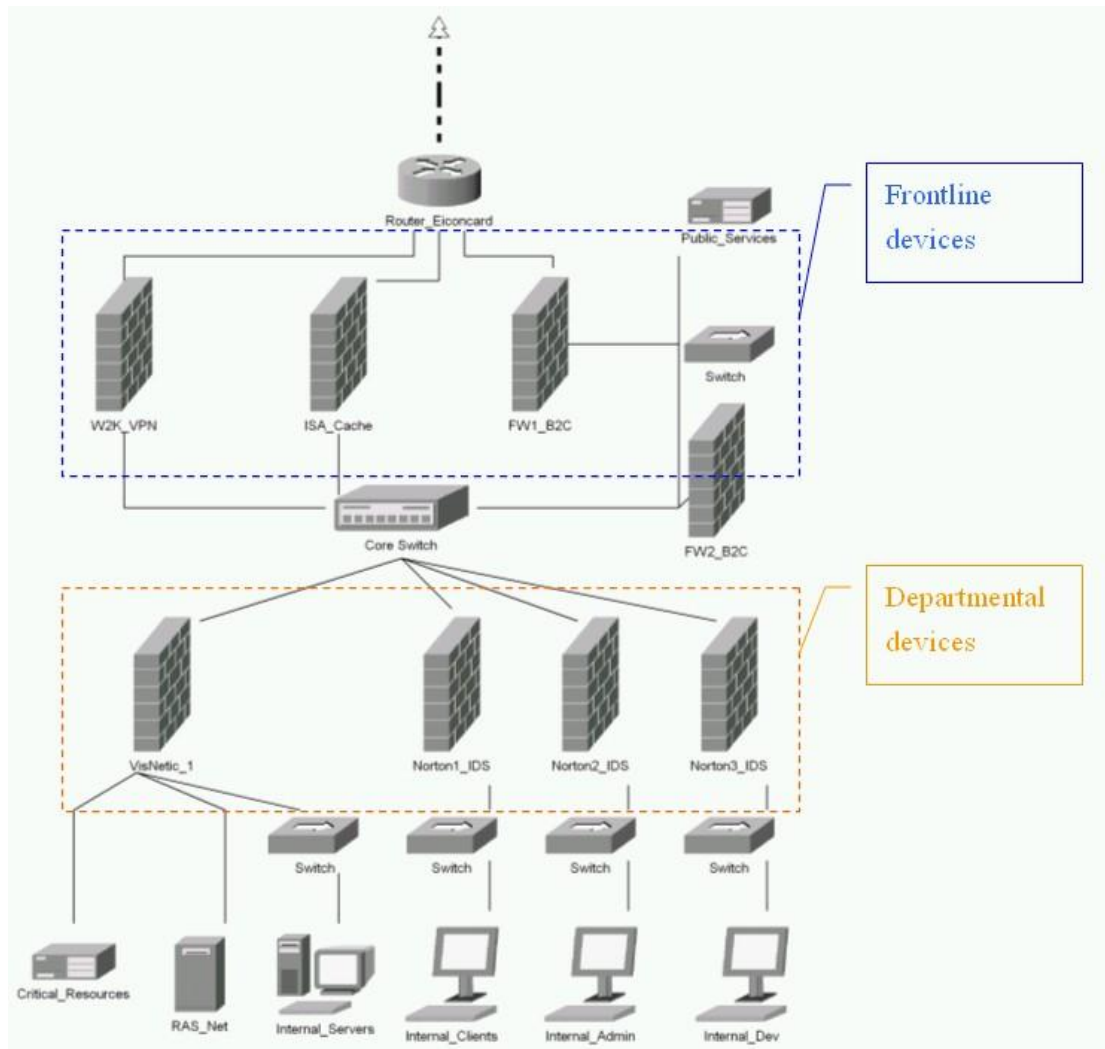
The reasons to use multiple devices are:

1,
On a truly secure network, multiple layers of firewall must be used. The proposed network security architecture for GIAC is designed based on the principle of "defense-in-depth", where security is applied in layers to make the life of hackers much harder than expected.

2,
Simplicity. Firewall technology can be as advanced and complicated as possible, but the underlying security rules and policies should not. Lance Spitzner in his article "Building Your Firewall Rulebase" repeatedly emphasizes the importance of

simplicity as the key to successful firewall implementation[1].

In order to make simple rulebase possible, we must divide the defense work into pieces and have these pieces distributed among multiple firewalls. With each firewall enforcing a smaller subset of the overall policies, the following benefits can be achieved:

- Reduce the complexity of each rulebase.
- Reduce the chance of mis-configuration and rule conflicts in each rulebase.
- Reduce the rulebase processing overhead on each firewall.
- Eliminate single point-of-failure.
- Easy troubleshooting.
- Scalability.

The above benefits cannot be obtained without paying a price. The tradeoffs are:

- Additional hardware have to be purchased.
- Additional maintenance works are expected.
- It can be argued that the more hardware involved, the higher the probability of hardware failure leading to network downtime.
- Some security administrators fear that the word "simplicity" means inferior technical skills.

There are always tradeoffs. I decided to go for a design which advocates Simplicity. In my design, I tried to have as few rules as possible being enforced at each firewall.

IP Infrastructure

Once the technical requirements have been defined, the GIAC network is segmented into multiple subnets for protection under different firewalls at different layers.

---

[1] http://www.enteract.com/~lspitz/rules.html

Subnets:

The GIAC network is segmented into the following subnets:

■ Core_Net: this is the subnet at which the external connections meet the internal connections.

■ Public_Services: hosting all the public services, including WWW, external email and external DNS. It is essentially a protected DMZ (Demilitarized Zone) which sits between the Internet and an internal network's line of defense under the protection of firewalls. This segment also houses an IDS to detect intrusion.

■ Internal_Clients: hosting all the in-house end user desktops. This group can actually be further segmented on an as needed basis.

■ Internal_Admin: hosting desktops for the mighty administrators.

■ Internal_Dev: hosting the in-house developers who need to make changes to the Ecommerce application and access the critical databases.

■ Internal_Servers: hosting the internal servers.

■ Critical_Resources: hosting the database application that is to be accessed by the external partners and suppliers.
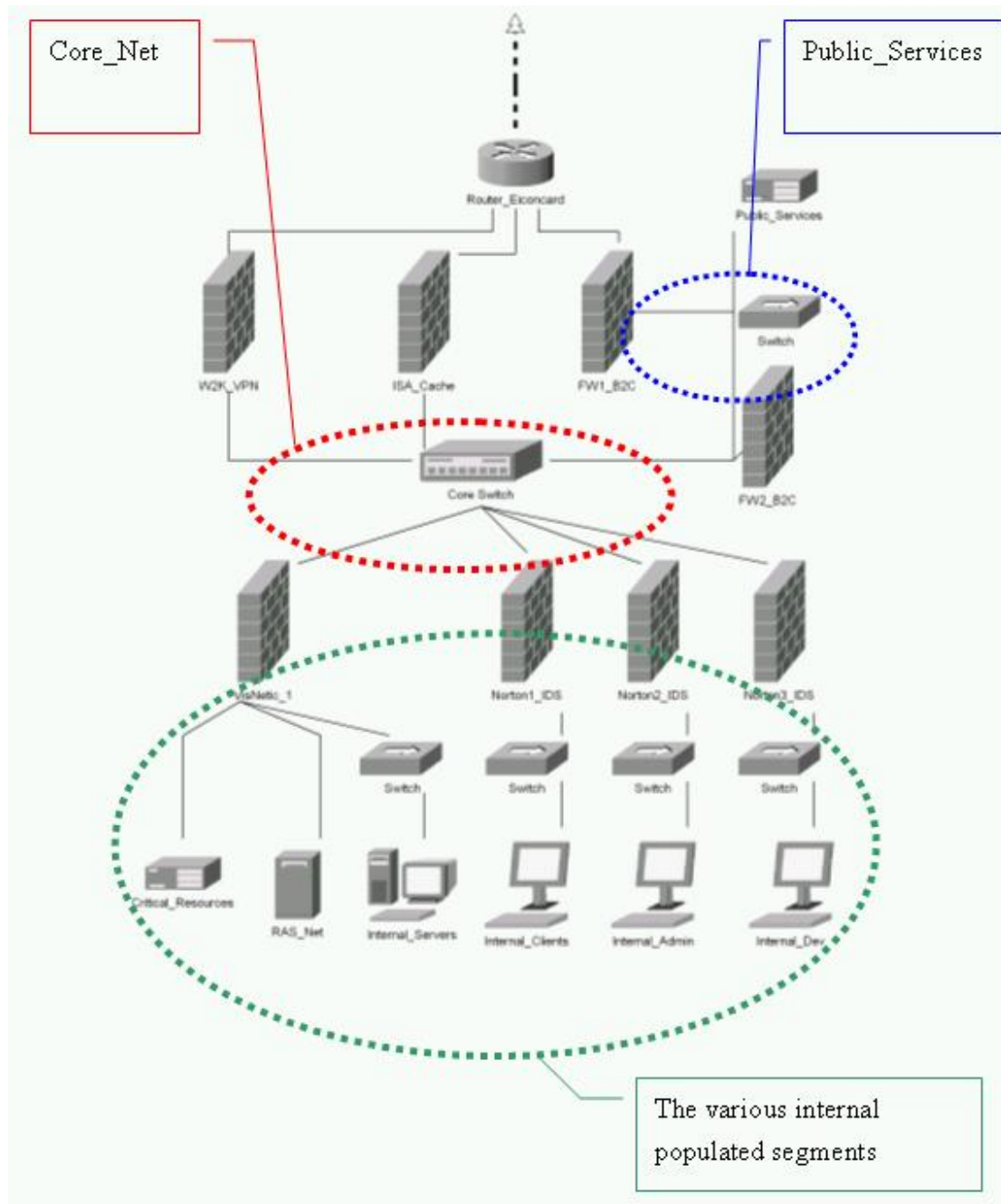
IP Settings:

The IP address scheme in this project is simplified for illustrating the connection configuration.

Core_Net (192.168.16.0)

Public_Services (192.168.8.0):
- WWW – 192.168.8.3 (NAT -> 192.168.7.8)

- Ext_DNS – 192.168.8.4 (NAT -> 192.168.7.9)
- Ext_SMTP – 192.168.8.5 (NAT -> 192.168.7.10)
- IDS – 192.168.8.6 (No NAT is needed, as the IDS is not published)

Internal_Clients (192.168.17.0) – In-house users should reside in this group. In fact, this group may be further segmented into different groups based on functions, departments, roles…etc. The majority of computers are window-based, with IP addresses statically assigned on each of them.

Internal_Servers (192.168.18.0)
- DNS Server – 192.168.18.3
- Email Server – 192.168.18.4
- Intranet Web Server - 192.168.18.7
- File Server - 192.168.18.8
- Print Server - 192.168.18.9
- Domain Controller 1 - 192.168.18.10
- Domain Controller 2 - 192.168.18.11

Internal_Admin (192.168.19.0)

Internal_Dev (192.168.20.0)

Critical_Resources (192.168.21.0):
- Database Application Server – 192.168.21.2

RAS_Net (192.168.22.0):
- RAS_Server – 192.168.22.2

Firewall & Routing Equipments

Overview:

The routers and firewalls used in this project are software based. The reasons to deploy software based solutions include:

- cost and availability
- flexibility of configurations

Layers of Protection:

In terms of security, the goal is to ensure that critical internal resources must have multiple layers of protection if being accessed from the "outside". In such a multi-layer architecture, firewalls of different brands/makes are used such that any vulnerability on any one of them won't render the entire solution breakable.

To ensure that the firewall systems themselves are secure, only local console logins are allowed. Login via the network (such as telnet) are entirely disabled. On a large and complex network, it is desirable to setup out-of-band channels for the centralized administration of these firewalls. On GIAC's relatively simple network, however, such approach may be too complicated and costly to implement.

Frontline/Primary Firewalls:

To protect the network against outside intrusion at the frontline, it is desirable to use name brand firewall software that has solid reputations. In the GIAC network, the frontline firewall on the B2C link is Check Point FW-1. We should always opt for using the latest versions of these software, but due to resource limitation, the FW-1 version being used is 4.0 (which is 2 years old already) running on NT Server 4.0.

Departmental Level Firewalls:

Firewalls at the departmental level include Norton Personal Firewall 2002 and Deerfield VisNetic. These firewall solutions provide additional layers of protection at much lower costs, making a defense-in-depth strategy possible cost effectively.

Equipment Guidelines:

In order to provide security, reliability and an acceptable level of performance, the computer hardware platforms must be dedicated – a firewall system should just act as a firewall and nothing else. The minimum recommended hardware requirements for the dedicated router/firewall platforms really depend on the actual use. When drafting the hardware requirements, the guidelines are:

- Routing and traffic inspection are CPU intensive. Dual-processor system is always recommended. Although many router/firewall products do not make use of SMP (Symmetric Multiprocessing, a computer architecture that makes multiple CPUs available to complete individual processes simultaneously), the operating systems (Windows NT, Windows 2000, Linux…etc) themselves can assign one processor to specialize in handling the OS stuff, thus freeing another processor to perform routing or traffic inspection.

- It is always true that more RAM is beneficial. When using Windows 2000 Server as the OS, 128MB RAM is the basic minimum, while 256MB RAM is the preferred baseline. Windows 2000 Professional is generally less demanding.

- RAID 1 disk mirror should be used for redundancy. Windows NT and Windows 2000 (as well as many Linux / Unix distributions) supports RAID 1 natively without the need to purchase additional hardware. The good thing about RAID 1 is that it can protect the OS itself, while RAID 5 cannot (I am talking about software RAID 5 here).

- Reserve sufficient drive space to accommodate the logs. These logs are to be backed up regularly just in case further analysis is required.

- Good quality 100BaseT NICs from reputable manufacturers (such as 3COM and Intel) are used. These cards are relatively stable and trouble-free in terms of installation and compatibility.

List of Equipments:

Below is a list of router and firewall equipments used in the GIAC network. The network diagram does not represent the "physical locations" of these equipments. In fact, a properly secured and climate controlled server room should be assigned for hosting these equipments. Physical security is as important as logical security in the real world.
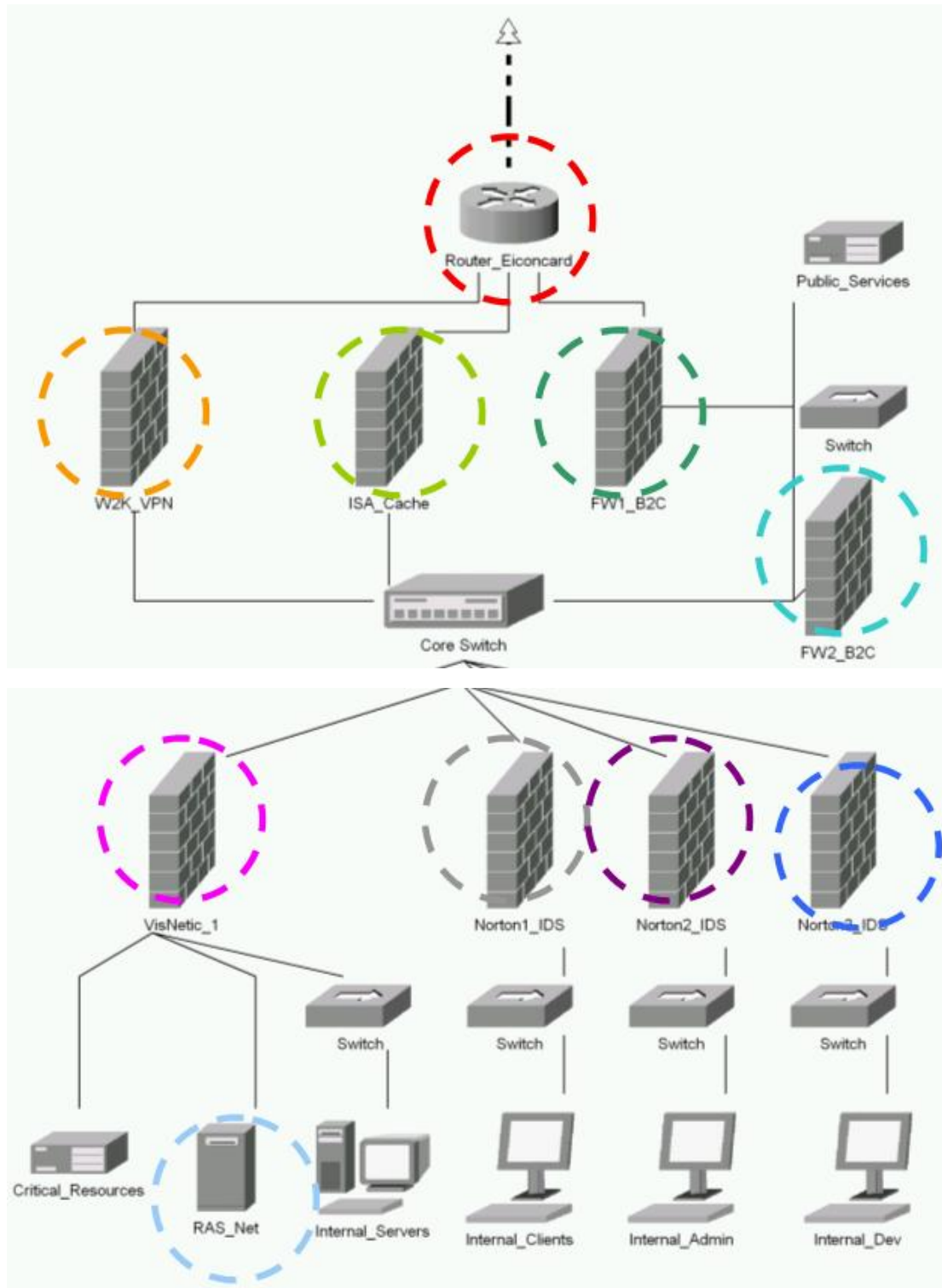
Router_Eiconcard:

- Border router for both the B2C link and the B2B link
- Platform: Platform: x86 based Windows 2000 Server equipped with a single

Eiconcard S92 dual WAN ports adaptor and three 100BaseT NICs.

■ Hardware: Dual Pentium-3 800MHZ, 384MB RAM, 20GB Disk Mirror, one WAN Adaptor (Eiconcard, supports 2 WAN ports) and three 100BaseT NICs.

FW1_B2C:

■ Frontline/Primary firewall on the B2C link against outside intrusion

■ Perform NAT to hide the IP addresses of the public service servers

■ Platform: x86 based NT Server 4.0 running Check Point FW-1 version 4.0

■ Hardware: Dual Pentium-3 800GHZ, 512MB RAM, 40GB Disk Mirror, two 100BaseT NICs.

FW2_B2C:

■ Second firewall on the B2C link against penetration

■ Platform: x86 based NT Server 4.0 running Check Point FW-1 version 4.0

■ Hardware: Single Pentium-3 800GHZ, 256MB RAM, 20GB Disk Mirror, two 100BaseT NICs.

Norton1_IDS:

■ Firewall protection for Internal_Clients

■ Intrusion Detection. Good intrusion detection necessitates predicting vulnerabilities using tools that continually monitor the network for threats.

■ Platform: x86 based Windows 2000 Professional running Norton Personal Firewall 2002

■ Hardware: Single Pentium-2 300MHZ, 192MB RAM, 4GB Disk Mirror, two 100BaseT NICs.

> ***Wait a minute! Norton PERSONAL Firewall? Are you serious?***
>
> *In fact, the name PERSONAL firewall is a bit misleading. Symantec positions the product as the choice for Small-to-Medium Enterprises rather than for pure home use. And, there are good reasons to use it in our design to protect the users:*
>
> ❑ *For the segments containing purely end users but no services, most risks come from the users' internet activities. They always bring in malicious codes and scripts, harmful applets and ActiveX controls. Norton Personal Firewall is specifically designed to protect the users against these internet risks.*
> ❑ *Its auto intruder blocking / auto update features make our life much easier.*
> ❑ *It has the lowest price tag, and does not require expensive server hardware to run.*

Norton2_IDS:

- Firewall protection for Internal_Admin
- Intrusion Detection
- Platform: x86 based Windows 2000 Professional running Norton Personal Firewall 2002
- Hardware: Single Pentium MMX 233MHZ, 128MB RAM, 4GB Disk Mirror, two 100BaseT NICs.

Norton3_IDS:

- Firewall protection for Internal_Dev
- Intrusion Detection
- Platform: x86 based Windows 2000 Professional running Norton Personal Firewall 2002
- Hardware: Single Pentium MMX 233MHZ, 128MB RAM, 4GB Disk Mirror, two 100BaseT NICs.

> *Why do we divide the entire user base into three different groups with each of them under the protection of different firewalls?*
>
> *The answer to this question is: we need to achieve separation of business functions:*
>
> ❑ *The administrators possess all the mighty privileges and tools for manipulating the entire network. It will be a disaster if their systems are compromised either by disgruntled employees or by external hackers.*
> ❑ *The developers possess all the codes and technology secrets for the ecommerce applications. It will be a disaster if this information is compromised. Again, disgruntled employees and external hackers are the potential sources of such threat.*
> ❑ *The clients usually make unintentional (and properly intentional yet amateur) troubles. These troubles are better to be contained within their own segment.*

VisNetic_1:

- Firewall protection for Internal_Servers, RAS_Net and Critical_Resources
- Platform: x86 based Windows 2000 Server running Deerfield VisNetic Firewall
- Hardware: Single Pentium-3 800MHZ, 256MB RAM, 20GB Disk Mirror, four 100BaseT NICs.

ISA_Cache:

- Proxy caching and firewall protection for outgoing internet traffic from Internal_Clients, Internal_Admin and Internal_Dev.
- Platform: x86 based Windows 2000 Server running Microsoft ISA Server Standard Edition
- Hardware: Single Pentium-4 1GHZ, 256MB RAM, 50GB Disk Mirror, two 100BaseT NICs.

W2K_VPN:

- VPN Gateway servicing inbound VPN connection requests from the external partners and suppliers

- Platform: x86 based Windows 2000 Server
- Hardware: Single Pentium-3 500MHZ, 256MB RAM, 20GB Disk Mirror, two 100BaseT NICs.

RAS_Server:

- RAS server servicing dial in clients
- Platform: x86 based Windows 2000 Server
- Hardware: Single Pentium-2 300MHZ, 192MB RAM, 8GB Disk Mirror, one 100BaseT NIC, five modems.

> ### *Why not combining VPN and Proxy into one single server?*
>
> *Instead of running VPN and Web proxy on the same server, we decide to have them run separately. The reason is performance and scalability. VPN encryption is CPU intensive. Although the connections for now are not overwhelming, its load is expected to grow sharply when GIAC expands. This is why it is better off to keep VPN on a separate computer.*

The exhibit below gives a bird-eye view of the GIAC security architecture:
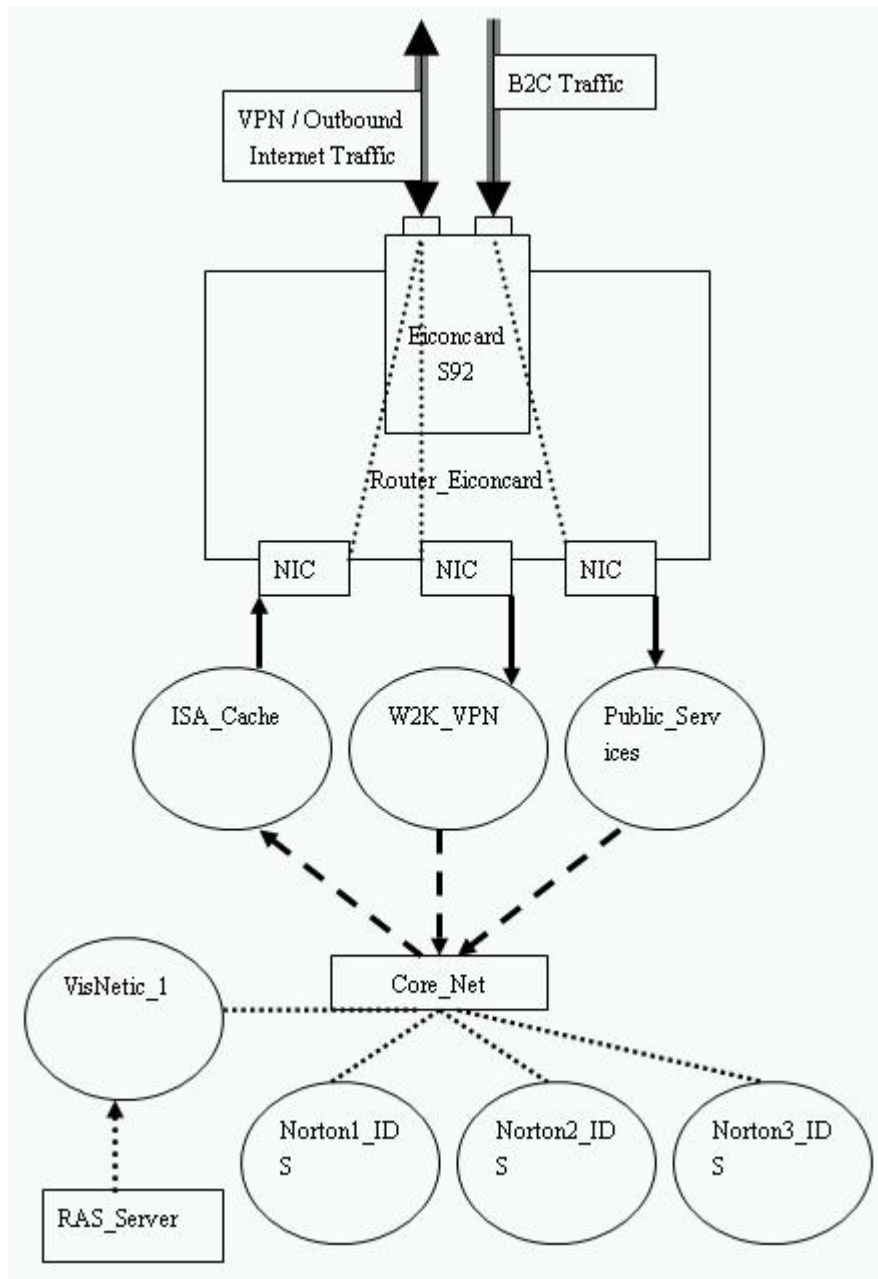
Equipments' IP Settings:

The IP address scheme in this project is simplified for illustrating the connection configuration. In the real world, some of these addresses are to be assigned by the ISP and are tailor masked.

Router_Eiconcard:

- 192.168.4.1 (to the internet)
- 192.168.5.1 (to ISA_Cache)

- 192.168.6.1 (to W2K_VPN)
- 192.168.7.1 (to FW1_B2C)

W2K_VPN:

- 192.168.6.2 (to Router_Eiconcard)
- 192.168.16.5 (to the core switch / Core_Net)

FW1_B2C:

- 192.168.7.2 (to Router_Eiconcard)
- 192.168.8.2 (to Public_Services)

FW2_B2C:

- 192.168.16.1 (to the core switch / Core_Net)
- 192.168.8.1 (to Public_Services)

Norton1_IDS:

- 192.168.16.2 (to the core switch / Core_Net)
- 192.168.17.1 (to Internal_Clients)

Norton2_IDS:

- 192.168.16.3 (to the core switch / Core_Net)
- 192.168.19.1 (to Internal_Admin)

Norton3_IDS:

- 192.168.16.4 (to the core switch / Core_Net)
- 192.168.20.1 (to Internal_Dev)

VisNetic_1:

- 192.168.16.6 (to the core switch / Core_Net)
- 192.168.18.1 (to Internal_Servers)
- 192.168.21.1 (to Critical_Resources)
- 192.168.22.1 (to RAS_Net)

ISA_Cache:

- 192.168.5.2 (to Router_Eiconcard)
- 192.168.16.7 (to the core switch / Core_Net)

RAS_Server:

■   192.168.22.2 (to RAS_Net)

Equipment Fault Tolerance and Redundancy:

Although it is possible to run the firewall/routing services on highly sophisticated cluster equipments, lower cost alternatives are possible. First of all, machine level fault tolerance can be established by using Disk Mirroring and UPS:

■   With Disk Mirroring, data is written to two duplicate disks simultaneously. If one of the disk drives fails, the system can instantly switch to the other disk without any loss of data nor downtime.

■   UPS (uninterruptible power supply) is a special kind of power supply that uses a battery to maintain power in the event of a power outage. It enables automated backup and shut down procedures in case there's a sudden power failure.

Another thing that can be done for redundancy is to maintain an identical system as a standby system for the most critical firewall and router implemented. This standby machine should have the exact same hardware and software configuration as the "original".

To implement a standby machine, the following steps are recommended:

1.   Complete the configuration of the "original" system.
2.   Backup the security/routing policy and object database as well as any other exportable security/routing settings to removable medias. Keep them in a safe and secure yet assessable place.
3.   Produce hard copy documents of the security/routing policy settings. Keep them in a safe and secure yet assessable place.
4.   Use a disk cloning utility such as the Norton Ghost utility to create an image of the entire system disk.
5.   Create the identical standby system by restoring the image to an identical computer.
6.   Test the standby system while the "original" is off.

Keep in mind, utility like Ghost will clone EVERYTHING, including the system's SID. This is perfectly ok as long as the original system and the standby system are

NOT going online at the same time. Remember, the standby system should be allowed to go online only when the "original" is offline.

Assignment 2

Define the GIAC Security Policy
Security Step-by-step Tutorial

Design Principle

As mentioned by Lance Spitzner in his article "Building Your Firewall Rulebase", *security policy defines what is to be enforced*[2].

The firewall is a tool for defining how the security policy is enforced. Before we implement any firewall solution, the security policy must first be clearly defined. As Lance said, the key to success is **simplicity**. Complicated policy gives room to mis-configuration.

Firewall rulebases follow and implement the defined security policies. For every rulebase, the principle is straight forward – anything not explicitly allowed by a rule is rejected by default. This way the rulebase can be kept as simple as possible without the need to introduce tons of complicated (and possibly conflicting) rules.

Layered Architecture

It is not possible to encompass protection of all sorts for every segment into a single firewall. The GIAC's network deploys a layered protection architecture, meaning different firewalls are implemented at different points of the network. The entire network is secured when the appropriate security policies are allocated to the appropriate firewall such that every corner of the network is secured.

To implement this security architecture, we need to:

1. define overall security policies for the enterprise based on its technical requirements
2. allocate enforcement duties to the firewalls
3. on every firewall, define specific rules and settings for policy enforcement

---

[2] http://www.enteract.com/~lspitz/rules.html

Overall Policy Objectives

For the GIAC project, the overall policy objectives are defined as follow:

- Policy Objective 1: The Public Services servers must be protected against outside intrusion attempts as much as possible. This policy is enforced at FW1_B2C.

- Policy Objective 2: Internal network is protected against outside intrusion from the B2C link should the Public Services segment be compromised. Computers in the public services area are not allowed to initiate connections to the other parts of the internal LAN. Such policy is enforced at FW2_B2C.

- Policy Objective 3: Public Services servers must be protected against tampering by the internal users while allowing client access, administrative maintenance or design updates. This policy is enforced at FW2_B2C.

- Policy Objective 4: Every internal network segments must be protected against tampering from the other internal segments. The relevant policies are enforced at Norton1_IDS, Norton2_IDS, Norton3_IDS, and VisNetic_1.

- Policy Objective 5: External partners and suppliers can access (via VPN) the Critical Resources database server via the standardized HTTP/HTTPS interface and do nothing else. The relevant policies are enforced at W2K_VPN and VisNetic_1.

- Policy Objective 6: Only authenticated staffs are allowed to log in via RAS. Such policies are enforced at the RAS Server. These RAS users, once logged in, can access the Internal Servers and the Public Services servers (and nothing else) from home or from trip via dial-in modems. The relevant policies are enforced at VisNetic_1.

Why do we disallow the RAS users to access their own desktops?

In GIAC, all resources are supposed to be stored in the servers. By restricting the RAS users to access only the servers, we are effectively encouraging them to save files in the servers rather than to keep local copies.

Why do we disallow the RAS users to access Critical_Resources?

In GIAC, the Critical_Resources segment contains server with critical database records. Since these records contain critical and sensitive information, access and updates must be handled seriously, and should be conducted only in the office. We definitely do not want these records to "leak" to the outside world via this channel.

■ Policy Objective 7: All internal users, as well as all servers from the Internal_Servers segment, are allowed to safely access the internet via proxying. Intrusion via this internet link must be blocked. The relevant policies are enforced at ISA_Cache, with additional protection such as Java /Active X blocking provided by Norton1_IDS, Norton2_IDS and Norton3_IDS.

Why do we allow the internal servers to access the internet via proxying?

In GIAC, there is no real need for servers in the Internal_Servers segment to reach the internet. However, many servers do rely on the internet as an update medium (for example, Microsoft Windows Update). Giving them the capability to connect allows certain degree of flexibility and productivity gain.

Why do we block Java and ActiveX for the users?

Java and ActiveX mainly run on the users' computers. They are client side

components that are often overlooked as potential threats[3].

< Anything not explicitly allowed are treated as PROHIBITED. >

The relationships between the firewalls/routers and the corresponding policy objectives are illustrated in the following exhibits:

---

[3] "Guidelines for Java, Javascript and ActiveX", Hack Proofing Your E-commerce Site, ISBN: 1-928994-27-X, http://www.syngress.com/catalog/sg_main.cfm?pid=1216
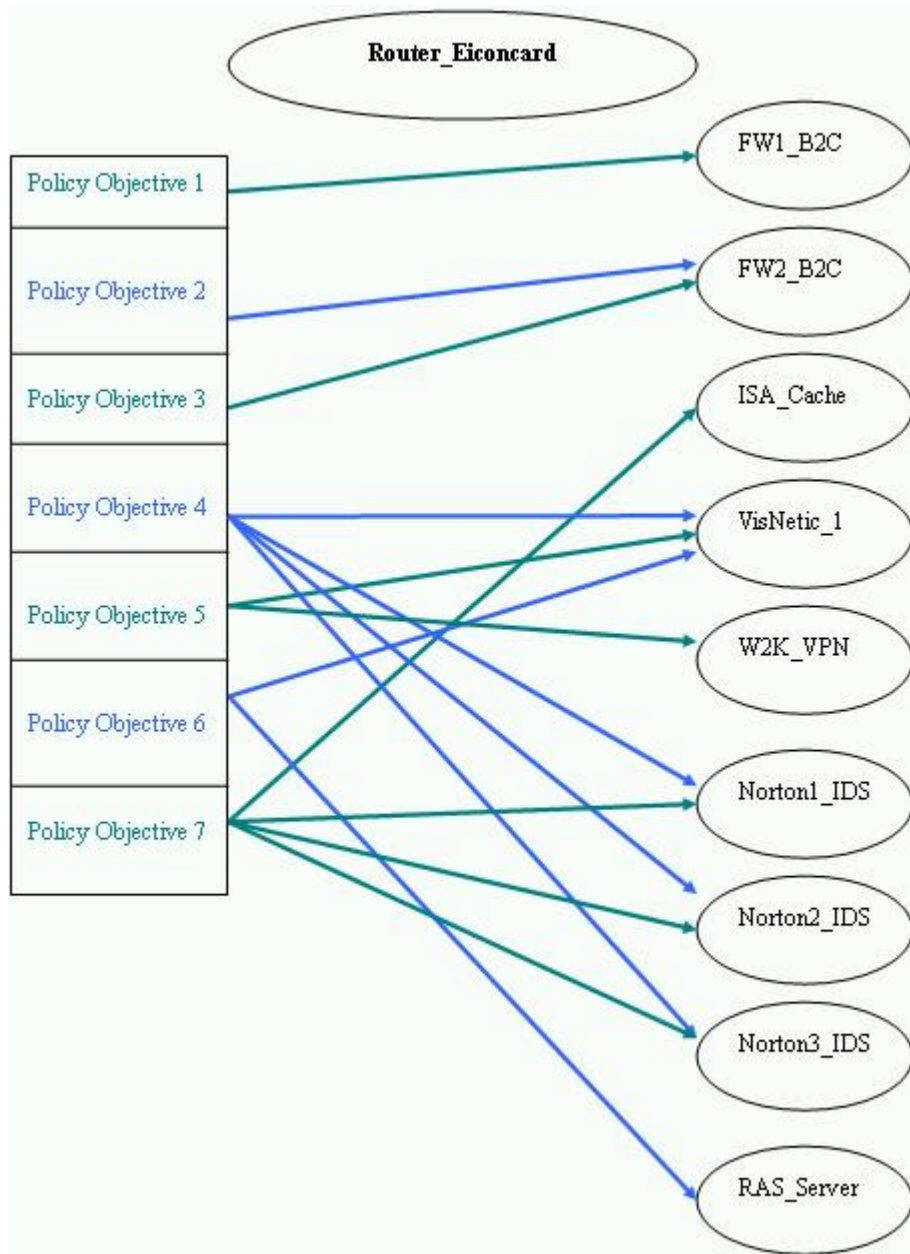
Local Policy Enforcement

Policies at Router_Eiconcard

1. Perform routing on the three traffic streams: B2B, B2C, INET
2. Packets coming in from the internet are inspected against spoofing.

Policies at FW1_B2C

1. Ecommerce web service – TCP port 80 (HTTP) and 443 (SSL) allowed IN
2. Email service for the external world – TCP port 25 (SMTP) allowed IN
3. DNS service for the external world – UDP port 53 (DNS request) allowed IN
4. Drop and log everything else

Policies at FW2_B2C

1, Ecommerce web service:
- Any traffic allowed from Internal_Admin.
- HTTP/HTTPS traffic allowed from Internal_Dev (Developers use HTTP/HTTPS based update method such as Frontpage Server extension).
- HTTP/HTTPS traffic allowed from Internal_Clients.
- HTTP/HTTPS traffic allowed from RAS_Net.

2, External email service:
- Any traffic allowed from Internal_Admin.
- SMTP traffic allowed from the internal email server for retrieving and sending emails to and from the outside world.

3, External DNS service:
- Any traffic allowed from Internal_Admin.
- DNS query traffic allowed from Internal_Dev.
- DNS query traffic allowed from Internal_Clients.
- DNS query traffic allowed from RAS_Net.

4, IDS:

- The IDS can alert Internal_Admin via SMTP.
- Snort (http://www.snort.org/) is an ideal IDS software for such purpose.
- To be secure, the IDS itself is hardened and is protected by a firewall service running on itself.
- The IDS has its own SMTP service solely for sending alerts - sending emails to the administrator's mailbox located in the internal email server.

5, Drop and log everything else.

Policies at ISA_Cache

1. Provide proxy service for internal clients accessing the internet. Protocols allowed include: HTTP, HTTPS, FTP, SMTP, POP3, IMAP, DNS, NNTP
2. Provide HTTP and FTP caching service for internal clients accessing the internet.
3. Allow outgoing PPTP traffic from internal PPP based VPN clients accessing external partners' VPN sites.
4. Prevent unauthorized users from accessing the proxy service.
5. Disallow any incoming requests from the outside world.
6. Disallow everything else.

Policies at VisNetic_1

1. Only Internal_Admin can freely access all segments behind this firewall with any protocol he/she likes.
2. External partners and suppliers can access only the Critical_Resources segment. Such access must originate from Core_Net via W2K_VPN, using HTTP and HTTPS as the protocols. Their access must be restricted by application level authentication and authorization.
3. Internal_Clients and Internal_Dev can access Internal_Servers with any protocol, although their access must be restricted by system level authentication and authorization.
4. Internal_Clients and Internal_Dev can access Critical_Resources only via HTTP and HTTPS. Their access must be restricted by application level authentication and authorization.

5. RAS users who connect via RAS_Net can access the Internal_Servers segment with any protocol, although their access must be restricted by system level authentication and authorization. Their access to Public_Services is subject to filtering at FW2_B2C.

6. Drop and log everything else.

Policies at W2K_VPN

1. Only PPTP connections from the legitimate external partners / suppliers are allowed.

2. No other inbound / outbound traffic types are allowed through this router. That means, drop and log everything else.

Policies at Norton1_IDS

1. No connection towards Internal_Clients can ever be initiated from any other segment (except from Internal_Admin).

2. Outbound access requests made by Internal_Clients are not restricted by this firewall, but by other firewalls on the network.

3. When the clients access the internet, Java and ActiveX codes are blocked.

4. Drop and log everything else.

Policies at Norton2_IDS

1. No connection towards Internal_Admin can ever be initiated from any other segment.

2. Outbound access requests made by Internal_Admin are not restricted by this firewall.

3. When the administrators access the internet, Java and ActiveX codes are blocked.

4. Drop and log everything else.

Policies at Norton3_IDS

1. No connection towards Internal_Dev can ever be initiated from any other

segment.

2. Outbound access requests made by Internal_Dev are not restricted by this firewall, but by other firewalls on the network.
3. When the developers access the internet, Java and ActiveX codes are blocked.
4. Drop and log everything else.

Policies at RAS_Server

1. Only legitimate users with the valid credentials and from the valid dialing locations are allowed to login.
2. Disallow everything else.

Products Preparation

To present a complete picture of the security architecture implementation, the security products in use as well as the steps taken to have them hardened are introduced here.

Eiconcard S92

According to www.eicon.com, Eiconcard S92 is an intelligent multi-protocol wide-area network interface card for PCI-bus based servers. It offers two Very High Speed Interface (VHSI) ports supporting line speeds of up to 2Mbps (T1/E1), and allows connection over a variety of WAN protocols such as X.25 or Frame Relay, over leased lines. It offloads the server from low level protocol processing tasks, resulting in a saving of valuable CPU resources[4].

The Eiconcard S92 works in conjunction with Eicon Networks' connectivity software, which runs smoothly on Windows 2000 Server. As a server-based router, the software extends the WAN capabilities of Microsoft Windows 2000 and provides support for IP on multiple WAN protocols.

For both performance and security concerns, the Windows 2000 configuration hosting Eiconcard should be optimized and hardened. The detail of doing so is introduced later in this document.

Check Point Firewall-1 on hardened Windows NT Server

Check Point (www.checkpoint.com) product has been selected due to its strong reputation in the industry since 1993. One primary selling point of Check Point FW-1 (http://www.checkpoint.com/products/security/firewall-1.html) is its' stateful

---

[4] http://www.eicon.com/worldwide/products/WAN/s92.htm

inspection technology. A form of dynamic packet filtering, stateful inspection works at the network layer and tracks each connection traversing all interfaces of the firewall to make sure they are valid.

Stateful inspection is "superior" as it examines not only the packet header but also the packet contents. Such inspection is done all the way up to the application layer, making it possible for filtering decisions to be made based on context that has been established by prior passed packets. As a measure against port scanning, stateful inspection firewalls always close off ports until connection to the specific port is requested.

For this project I used FW-1 version 4.0 for x86, which is not current but is what I have on hand. It runs on Windows NT Server 4.0. To make this firewall system truly secure, the things that need to be done are:

■   Hardening NT itself – apply all the latest service packs, patches and fixes; and disable all the unnecessary services and components.
■   Securing FW-1 – again, apply all the latest patches and fixes for version 4.

Hardening the NT Installation

According to CERT's NT configuration guidelines, there are two types of patches from Microsoft: Service Packs and Hotfixes. Service packs are for patching a wide range of vulnerabilities and bugs, while hotfixes are released more frequently than service packs and are for patching more specific problems[5].

Keep in mind though, that service packs are cumulative, meaning we only need to install the latest Service Pack. For fixes, however, we need to determine what to install (as we won't need all of them). **Service Pack must be installed before the Hotfixes.**

We may access all these service packs and updates from a central location: http://www.microsoft.com/ntserver/nts/downloads/default.asp#RecommendedUpdates.

---

[5]   http://www.cert.org/tech_tips/win_configuration_guidelines.html

As of the time of this writing, the latest service pack available for NT Server 4 is version 6a. We may also selectively apply the available hotfixes (now being referred to by Microsoft as "security updates").

Fine Tuning the NT Configuration

Stefan Norberg in his article "Building a Windows NT bastion host in practice" outlines several major steps to armor a general NT installation[6]. Some of these steps can be applied in our firewall installation, including:

- Remove unused network services.
- Disable unused services.
- Disable NetBIOS.
- Remove unused and potentially dangerous components.
- Encrypt the system accounts database.
- Strengthen the account and audit settings.

Note that:
- IIS has not been installed at the first place. There is no need to have IIS running on a firewall system.
- IP was the only protocol selected during system installation.
- NTFS is the only file system on the computer. FAT is not secure, and is not to be considered at all.

Step 1 – Remove unused network services

In our system, the following network services (which have been installed by default) are removed:

- Workstation (which in turn removes Computer Browser)
- NetBIOS Interface

---

[6] http://secinf.net/info/nt/ntbastion/

- RPC Configuration
- Server

FW-1 can function perfectly even without these services. One issue to consider is whether to install and use RIP for IP. For FW-1 to function correctly as a firewall gateway, routing must be properly configured on NT. Static routes are always safe and efficient, but can be complex to configure (it all depends on how complicated the network environment is). Using RIP on the firewall system can make life easier at the expense of very little performance overhead and a very limited (if not exist) security exposure. The security exposure is next to none if we remember to configure the border router to screen and block all RIP traffics.

Step 2 - Disable unused services

In our system, the following system services (which have been installed by default) are disabled:

- DHCP Client
- License Logging Service
- Network DDE DSDM
- Remote Procedure Call (RPC) Service
- Schedule
- Spooler
- TCP/IP NetBIOS Helper
- Telephony Service

Step 3 – Disable NetBIOS.

The goal is to get rid of all listeners on the NetBIOS ports. This can be done by disable the WINS client bindings of all NICs.
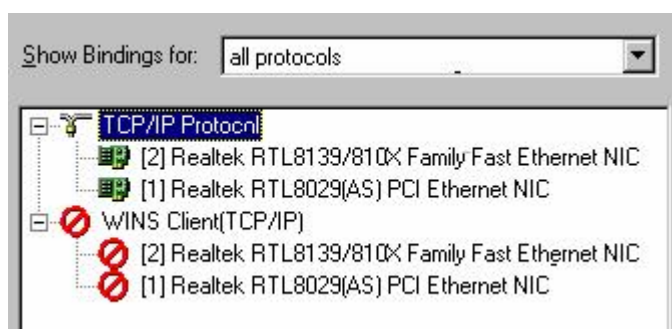
Step 4 - Remove unused and potentially dangerous components.

The "dangerous" components as listed in the article "Technical Reference: NT Server 4.0 Hardening Guide" are:

"xcopy.exe, wscript.exe, cscript.exe, net.exe, ftp.exe, telnet.exe, arp.exe, edlin.exe, ping.exe, route.exe, at.exe, finger.exe, posix.exe, rsh.exe, atsvc.exe, qbasic.exe, runonce.exe, syskey.exe, cacls.exe, ipconfig.exe, rcp.exe, secfixup.exe, nbtstat.exe, rdisk.exe, debug.exe, regedt32.exe, regedit.exe, edit.com, netstat.exe, tracert.exe, NSLOOKUP.exe, rexec.exe, cmd.exe, NSLOOKUP.exe, tftp.exe, command.com"[7]

In fact, we do not need to have them disappeared. However, it is a good idea to hide them. We may do this by taking them away from their original locations and place them in a special directory protected by fine tuned NTFS ACL settings.

Step 5 - Encrypt the system accounts database.

With the help of the syskey.exe utility, the SAM can be protected against password cracking attacks. Below is an extract of the Microsoft KB article Q143475 on syskey:

"The Windows NT Server 4.0 System Key hotfix provides the capability to use strong encryption techniques to increase protection of account password information stored in the registry by the Security Account Manager (SAM). Windows NT Server stores user account information, including a derivative of the user account password, in a secure portion of the Registry protected by access control and an obfuscation function. The account information in the Registry is only accessible to members of the

---

[7] http://screamer.mobrien.com/Manuals/MPRM_group/security.htm

Administrators group. Windows NT Server, like other operating systems, allows privileged users who are administrators access to all resources in the system. For installations that want enhanced security, strong encryption of account password derivative information provides an additional level of security to prevent Administrators from intentionally or unintentionally accessing password derivatives using Registry programming interfaces.

This file has been posted to the following Internet location:

ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/nt40/hotfixes-postsp2/sec-fix/"[8]

Step 6 - Strengthen the account and audit settings.

This is the step that I add to the list based on information provided by the article "Technical Reference: NT Server 4.0 Hardening Guide"[9].

An ideal password policy should include the elements listed below:

- Enforce password uniqueness by remembering last passwords 6
- Minimum password age: 2
- Maximum password age: 42
- Minimum password length: 10
- Complex passwords: Enabled
- User must logon to change password: Enabled
- Account lockout policy Account lockout count: 5
- Lockout account time forever Reset lockout count after: 720 minutes

"Complex passwords" requires that you deploy passfilt.dll, a special DLL file that comes with the NT service packs. Below is an extract of the description of this file from the KB article 161990:

"Microsoft Windows NT 4.0 Service Pack 2 introduces a new DLL file (Passfilt.dll) that lets you enforce stronger password requirements for users. Passfilt.dll provides

---

[8] http://support.microsoft.com/default.aspx?scid=kb;EN-US;q143475
[9] http://screamer.mobrien.com/Manuals/MPRM_group/security.htm

enhanced security against "password guessing" or "dictionary attacks" by outside intruders. ...The Passfilt.dll file implements the following password policy:

■ *Passwords must be at least six (6) characters long.*

■ *Passwords must contain characters from at least three (3) of the following four (4) classes:*

1.	*English upper case letters*	*A, B, C, ... Z*
2.	*English lower case letters*	*a, b, c, ... z*
3.	*Westernized Arabic numerals*	*0, 1, 2, ... 9*
4.	*Non-alphanumeric ("special characters") such as punctuation symbols*	

■ *Passwords may not contain your user name or any part of your full name.*

These requirements are hard-coded in the Passfilt.dll file and cannot be changed through the user interface or registry. If you wish to raise or lower these requirements, you must write your own .dll and implement it in the same fashion as the Microsoft version that is available with Windows NT 4.0 Service Pack 2.''[10]

An ideal audit policy should include the elements below:

■ Audit account management Success: Failure

■ Audit logon events Success: Failure

■ Audit object access: Failure

■ Audit policy change Success: Failure

■ Audit privilege use: Failure

■ Audit process tracking: No auditing

■ Audit system events Success: Failure

Additionally, remove any unnecessary user accounts. In theory, a single user account for the administrator is sufficient. Rename this account to something hard to guess. Thoroughly check the system's permission settings and ensure that no one else except the renamed administrator can have access.

FINALLY, do not forget to tighten the file system ACL settings. The policy files and the log files should not be accessible to the general users or any unauthorized service.

---

[10] http://support.microsoft.com/default.aspx?scid=kb;EN-US;q161990

A Clean FW-1 Installation

A clean FW-1 installation gives a good start. For our project, every FW-1 system uses two 100MBit NICs. Below is a point form summary of the installation process:

1. From the installation CD, install only Firewall-1 and the User Interface.
2. Choose the VPN-1 and Firewall-1 SINGLE GATEWAY installation.
3. Install the following GUIs: Security Policy, Log Viewer, System Status
4. Configure a single administrator account with Read/Write privileges.
5. Do not configure to allow remote GUI to connect. The GUI must be run from the same local machine.
6. Allow FW-1 to control IP Forwarding. This will ensure that no traffic can pass through the system before FW-1 is up and running. This is especially useful in a situation where the server is started but the Firewall services have not finished loading.
7. Ensure that the FW-1 service is to be started automatically everytime the system starts by checking Control Panel – Services.

Securing the FW-1 Installation

Nothing is perfect. FW-1 version 4.0m and 4.1 both suffer from bugs and vulnerabilities. Below is a list of version 4.0 vulnerabilities extracted from SecurityFocus[11]:

■ 2002-03-08: Check Point FW-1 SecuClient/SecuRemote Client Design Vulnerability
■ 2002-02-19: Multiple Vendor HTTP CONNECT TCP Tunnel Vulnerability
■ 2001-09-12: Check Point Firewall-1 GUI Log Viewer Vulnerability
■ 2001-09-08: Check Point Firewall-1 Policyname Temporary File Creation Vulnerability
■ 2001-09-08: Check Point Firewall-1 GUI Client Log Viewer Symbolic Link Vulnerability
■ 2001-07-18: Check Point Firewall-1 SecureRemote Network Information Leak Vulnerability

---

[11] http://online.securityfocus.com/cgi-bin/vulns.pl

- 2000-11-01:   Check Point Firewall-1 Valid Username Vulnerability
- 2000-08-15:   Check Point Firewall-1 Session Agent Dictionary Attack Vulnerability
- 2000-08-02:   Check Point Firewall-1 Unauthorized RSH/REXEC Connection Vulnerability
- 2000-07-05:   Check Point Firewall-1 Spoofed Source Denial of Service Vulnerability
- 2000-06-30:   Check Point Firewall-1 SMTP Resource Exhaustion Vulnerability
- 2000-06-06:   Check Point Firewall-1 Fragmented Packets DoS Vulnerability
- 2000-03-11:   Check Point Firewall-1 Internal Address Leakage Vulnerability
- 2000-03-10:   Multiple Firewall Vendor FTP "ALG" Client Vulnerability
- 2000-02-09:   Multiple Firewall Vendor FTP Server Vulnerability
- 1999-10-20:   Check Point Firewall-1 LDAP Authentication Vulnerability
- 1999-08-09:   Firewall-1 Port 0 Denial of Service Vulnerability
- 1999-07-29:   FireWall-1, FloodGate-1, VPN-1 Table Saturation Denial of Service Vulnerability
- 1998-09-24:   Check Point Firewall-1 Session Agent Impersonation Vulnerability

Some recent major FW-1 bugs and vulnerabilities are described in the following web sites:

- http://www.tla.ch/TLA/NEWS/2000sec/20000731Check PointTUV.htm
- http://www.securiteam.com/securitynews/FW-1_IP_Fragmentation_vulnerability __remote_DoS_.html

Check Point offers service packs and hotfixes on a regular basis. It is important for you to install the latest of these service packs and hotfixes to secure your FW-1 installation. In order to obtain these software you must subscribe to Check Point's support program, which is available at http://www.checkpoint.com/techsupport/downloads/downloads.html.

As of the time of this writing, the latest service pack available for FW-1 version 4.0 is SP8.

Hardened Windows 2000

Perfecting the Windows 2000 Installation

First of all, install the latest service pack. At the time of this writing, SP2 is the latest available version. In fact, ISA will not install unless you have applied SP1 at the least.

Microsoft offers Windows 2000 service packs via this URL:
http://www.microsoft.com/windows2000/downloads/servicepacks/default.asp
Additionally, the security updates available at
http://www.microsoft.com/windows2000/downloads/security/default.asp should be applied.

Hardening the Configuration

The basic ideas behind the hardening strategy are always the same:

■ Remove unused network services.
■ Disable NetBIOS.
■ Configure IP Routing.
■ Disable unused services.
■ Strengthen the account and audit settings.
■ Remove unused and potentially dangerous components.
■ Go through all the file system permission settings.

Windows 2000 natively encrypts its account database, avoiding the need to manually run syskey. Philip Cox in his article "Hardening Windows 2000" does suggest that we further run Syskey to enforce the use of manual password entry to access the decryption key[12].

---

[12] http://www.sys-exp.com/win2k/HardenWin2K.html

Step 1 - Remove unused network services.

TCP/IP should be the only network service attached to each NIC.

Step 2 - Disable NetBIOS.

In the WINS section of each NIC's Advanced IP settings, deselect the "Enable LMHOSTS lookup" option, and choose the "Disable NetBIOS over TCP/IP" option.

Step 3 - Configure IP Routing.

This requires that we use the Routing and Remote Access MMC snap in (accessible from the Administrative Tools menu). For each routing interface (the NIC), there is no need to enable router discovery nor any filter. All that we want is for the multiple NICs on the same system to communicate with each other.

(Windows 2000 Professional supports only static routing, and does not provide the rich RRAS interface.)

By default, no routing protocol is used. Manually defining static routes can be time consuming, so a routing protocol is recommended. Windows 2000 supports RIP V2, which is simple and is less costly (in terms of processing power) than OSPF.

To use RIP, one must manually right click on "General" and choose "New Routing Protocol". Each participating NIC must then be manually selected for use by RIP.
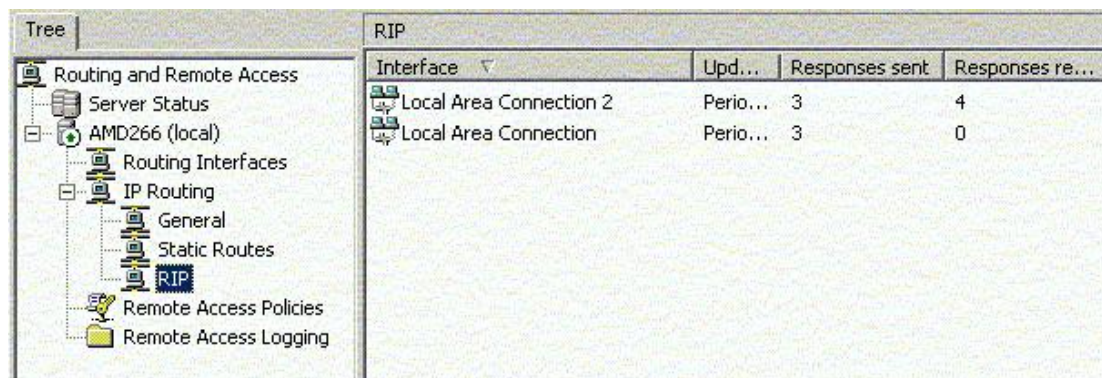
For security reason, we want to log as much information on RIP as possible. Also, we should restrict RIP from accepting announcements. In our project, the system should only accept announcement from our central router and no one else.
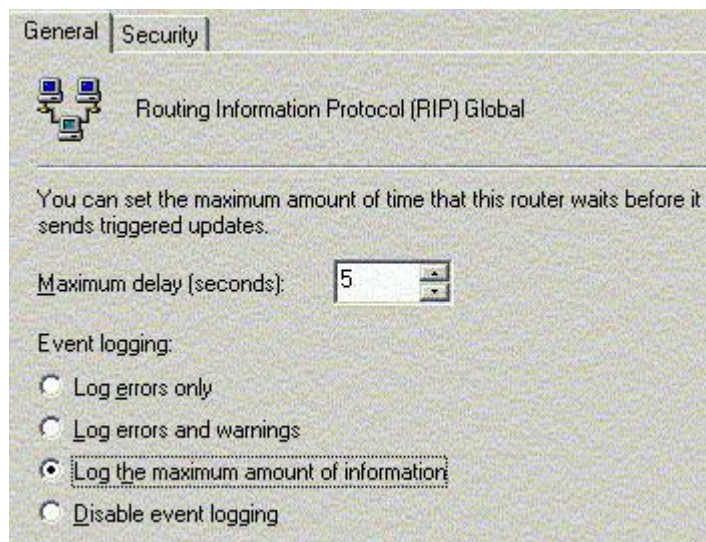
Step 4 - Disable unused services.

There are tons of Windows 2000 services loaded by default. However, most of them are not needed and should be disabled.

Philip Cox (above) suggests that the minimum services required to run the system are:

- DNS Client
- EventLog
- Logical Disk Manager
- Plug and Play
- Protected Storage
- Security Accounts Manager

For our purpose, the following additional services are to be retained:

- Network Connections

- Routing and Remote Access
- Workstation
- Server

The reason we need to keep the Workstation service and the Server service is that without them, the RRAS MMC snap-in will not work properly.

Step 5 - Strengthen the account and audit settings.

The ideal policies as suggested by Philip Cox (above) include:

Password Policies:
- Enforce Password History: Enabled (recommended value is 5)
- Maximum Password Age: Enabled (recommended value is 60)
- Minimum Password Age: Enabled (recommended value is 5)
- Passwords Must Meet Complexity Requirements: Enabled
- Store Password Using Reversible Encryption: Disabled

Account Lockout Policies:
- Account Lockout Threshold: Enabled (recommended value is 5)
- Account Lockout Duration: Enabled (recommended value is 30)
- Reset Account Lockout Threshold After: Disabled (recommended manual reset of accounts)

Audit Policy (Audit success and failure for the following audit categories):
- Audit Account Logon Events
- Audit Account Management
- Audit Logon Events
- Audit Policy Change
- Audit System Events

Refer to http://www.sys-exp.com/win2k/hardenW2K12.pdf for Philip Cox's full article.

Step 6 - Remove unused and potentially dangerous components.

The OS2 and Posix subsystems are obsolete and useless in our context. They can be removed using the method suggested by Philip Cox (above):

"... you can remove the OS2 and Posix registry values from the HKLM\System\CurrentControlSet\Control\SessionManager\SubSystems registry key. Then delete the associated files (os2*, posix*, and psx*) in the DLL cache directory, then from %systemroot%\System32 (otherwise windows file protection will immediately replace them)."[13]

Also, the following commands should either be relocated to some other locations or to be tightened up with stronger ACL settings. You do not want them to be accessed and used by the hackers:

- arp.exe
- at.exe
- atsvc.exe
- attrib.exe
- cacls.exe
- clipsrv.exe
- cmd.exe
- command.com
- cscript.exe
- debug.exe
- dialer.exe
- edit.com
- edlin.exe
- finger.exe
- ftp.exe
- hypertrm.exe
- ipconfig.exe
- nbtstat.exe

---

[13] http://www.sys-exp.com/win2k/hardenW2K12.pdf

- net.exe
- netstat.exe
- NSLOOKUP.exe
- ping.exe
- ping.exe
- posix.exe
- qbasic.exe
- rcp.exe
- rdisk.exe
- regedit.exe
- regedt32.exe
- rexec.exe
- route.exe
- rsh.exe
- runonce.exe
- secfixup.exe
- sysedit.exe
- syskey.exe
- telnet.exe
- tftp.exe
- tracert.exe
- wscript.exe
- xcopy.exe

Refer to http://www.sys-exp.com/win2k/hardenW2K12.pdf for Philip Cox's full article.

Step 7 – Go through the file system permission settings.

This assumes that only NTFS is deployed. FAT is insecure and is not to be used.

"Short for NT File System, one of the file system for the Windows NT operating system (Windows NT also supports the FAT file system). NTFS has features to improve reliability, such as transaction logs to help recover from disk failures. To control access to files, you can set permissions for directories and/or individual files. NTFS

files are not accessible from other operating systems such as DOS." (from webopedia.com[14]).

Be especially careful on the "Everyone" group. I would recommend that this group be removed from every ACL entry unless the removal would cause conflicts with the software running on the system (in our case this kind of "conflict" is highly unlikely).

Vulnerabilities

Windows 2000 is full of vulnerabilities (although many of them are IIS related)! A query made in the CERT site can retrieve many results:

http://www.cert.org/nav/index_red.html

It is recommended that this site be regularly visited to keep ourselves informed about the latest vulnerabilities.

Norton Firewall 2002

Norton Personal Firewall 2002 is available at http://www.symantec.com/sabu/nis/npf/ and is classified by Symantec as a firewall tool for small business rather than simply for personal use.

More information about this product is available at http://www.symantec.com/sabu/nis/npf/features.html . We will have it runs on Windows 2000 Server.

Configure Norton Firewall

After the Windows 2000 server is properly prepared and hardened, the firewall can be installed. It is vital for internet connectivity to be available at the time of installation so that LiveUpdate can be run. LiveUpdate is a service feature provided by Symantec for real time application of fixes, patches and updates. It requires connections to be made to Symantec's corporate site.

---

[14] http://www.webopedia.com/TERM/N/NTFS.html

For maximum protection, the firewall should be configured to run automatically at system startup. For the machine that runs Norton Firewall to protect the network behind it, routing must be configured. Windows 2000 Professional supports only static routing (v.s. dynamic routing in Windows 2000 Server). So, the proper route entries must be added manually via the route add command.

"Route Add adds routes to the table. Route Delete removes routes from the host's routing table. Routes added to a routing table are not made persistent unless the -p switch is specified. Non-persistent routes only last until the computer is restarted or until the interface is deactivated. The interface can be deactivated when the plug-and-play interface is unplugged (such as for laptops and hot-swap PCs), when the wire is removed from the media card (if the adapter supports media fault sensing), or when the interface is manually disconnected from the adapter in the Network and Dial-up Connections folder." (from Windows 2000 Server Resource Kit TCP/IP Core Networking Guide[15]).

Vulnerabilities

So far we did not find any vulnerability information on this product. It could be because it is too new (or that it is never a target of the hackers out there?).

Deerfield VisNetic Firewall

According to Deerfield,

"VisNetic Firewall is a stateful packet level firewall solution built to protect Windows-based Servers, stand alone PCs, and LAN workstations not currently protected by a firewall. VisNetic Firewall is more secure than application-based personal firewalls, yet less expensive than high-end firewalls, providing

---

[15]

http://www.amazon.com/exec/obidos/ASIN/1572318058/qid=1018718363/sr=1-1/ref=sr_1_1/104-955 7570-0347903

peace-of-mind through comprehensive intrusion protection."[16]

VisNetic is designed for business network. It provides a powerful yet flexible interface for defining the various filters and rules. At the time of this writing the current version of VisNetic Firewall is 1.0.2. No patch nor update has been announced yet. More information about this product is available at: http://www.deerfield.com/products/visnetic_firewall/

We use VisNetic Firewall to protect our internal servers. It operates on a Windows 2000 Server that runs RRAS and performs LAN routing. The steps to harden Windows 2000 are covered in detail in the previous sections. For VisNetic, the settings below are essential in securing the firewall itself:

Enlarge the log file:

The default size of 10MB may not be enough if we want to log everything. 50MB or larger is strongly recommended.

Configure the statuses:

Ensure that VisNetic will be started automatically everytime the system goes up:

---

[16] http://www.deerfield.com/products/visnetic_firewall/
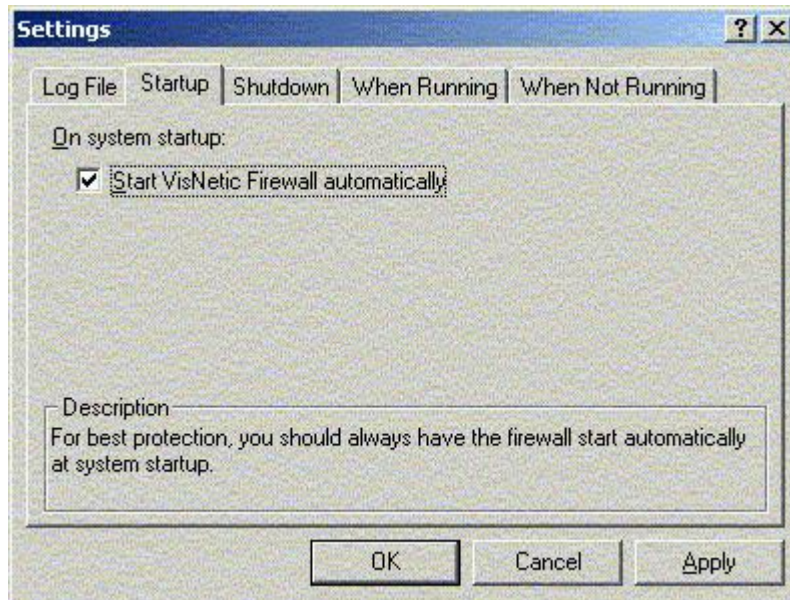
When running, the firewall must be in the Filter state.
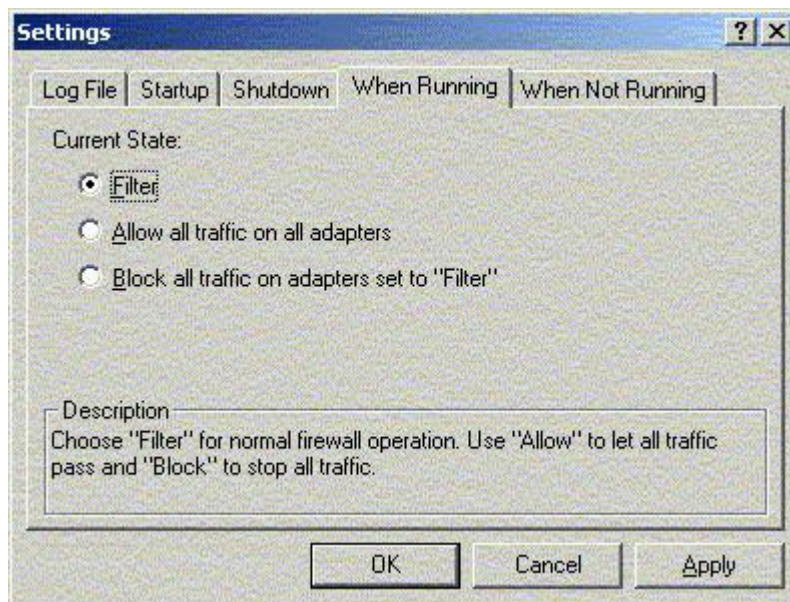
When the firewall service is not running (or is not YET started), all traffic should be blocked.
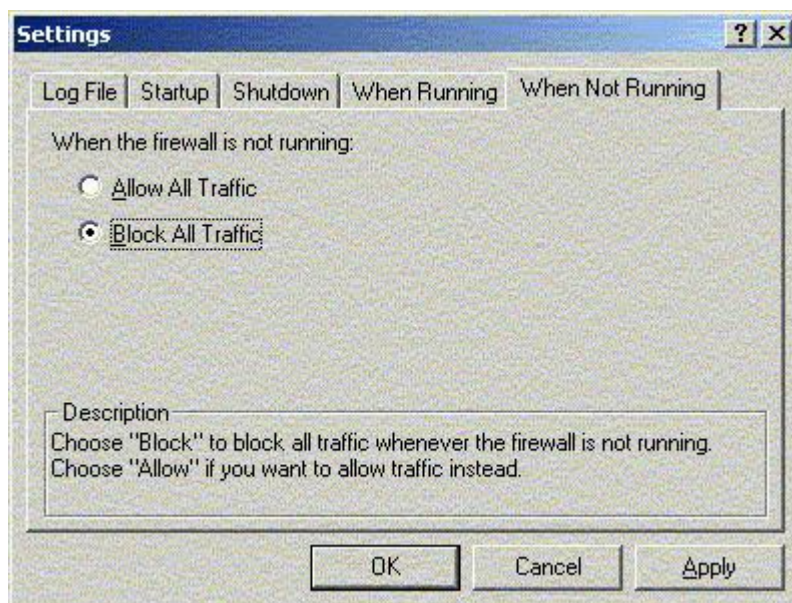
Vulnerabilities

Same as for Norton Firewall, we have not been able to identify any vulnerability for this product. This is likely due to the fact that this product is not as popular as their high end counterparts, thus is not the common target of attack (or that the attacks are not worth to be publicized).

Microsoft ISA Server

According to Microsoft,

"Microsoft Internet Security and Acceleration (ISA) Server 2000 is an extensible enterprise firewall and Web cache server that integrates with the Microsoft Windows® 2000 operating system for policy-based security, as well as accelerating and managing internetworking. ISA Server provides two tightly integrated modes—a multilayer firewall and a high-performance Web cache server. The firewall provides filtering at the packet, circuit, and application layer, stateful inspection to examine

data crossing the firewall, control of access policy, and routing of traffic. The cache improves network performance and enhances the end-user experience by storing frequently requested Web content. The firewall and cache can be deployed separately on dedicated servers or integrated on the same computer."[17]

The reason ISA Server is used in the GIAC network for:

- enhance performance – it can act as a proxy caching server for the internal clients, thus enhancing the client's internet browsing performance
- protect – it has advanced stateful inspection technology for protecting the network

The ISA Server edition that we use is the Standard Edition. And since it runs on Windows 2000 Server, it is necessary for us to secure the Windows 2000 installation first before deploying ISA.

Perfecting the Windows 2000 Installation

First of all, install the latest service pack. At the time of this writing, SP2 is the latest available version. In fact, ISA will not install unless you have applied SP1 at the least.

Microsoft offers Windows 2000 service packs via this URL:
http://www.microsoft.com/windows2000/downloads/servicepacks/default.asp
Additionally, the security updates available at
http://www.microsoft.com/windows2000/downloads/security/default.asp should be applied.

Hardening the Configuration

ISA Server includes a Security Configuration Wizard for hardening the Windows 2000 installation. Before invoking ISA for this purpose, apply all the available service packs and updates.

---

[17] http://www.microsoft.com/isaserver/evaluation/productguide.asp

Available at http://www.microsoft.com/isaserver/downloads/sp1.asp,
"Internet Security and Acceleration (ISA) Server 2000 Service Pack 1 (SP1) provides the latest updates to ISA Server and provides an even higher level of reliability and stability to customers. Microsoft strongly encourages customers to install SP1 on all computers running ISA Server."[18]

According to Microsoft, ISA Server SP1 includes all hot fixes issued since ISA Server was released to manufacturing, fixes for common issues reported by customers through Microsoft Product Support Services (PSS) as well as fixes recommended through an audit by third-party security experts.

Once the service pack is applied, we can invoke the Security Configuration Wizard and start hardening Windows 2000 Server. Of the three different security levels, choose "Dedicated" to produce the most secure firewall system.

---

[18] http://www.microsoft.com/isaserver/downloads/sp1.asp
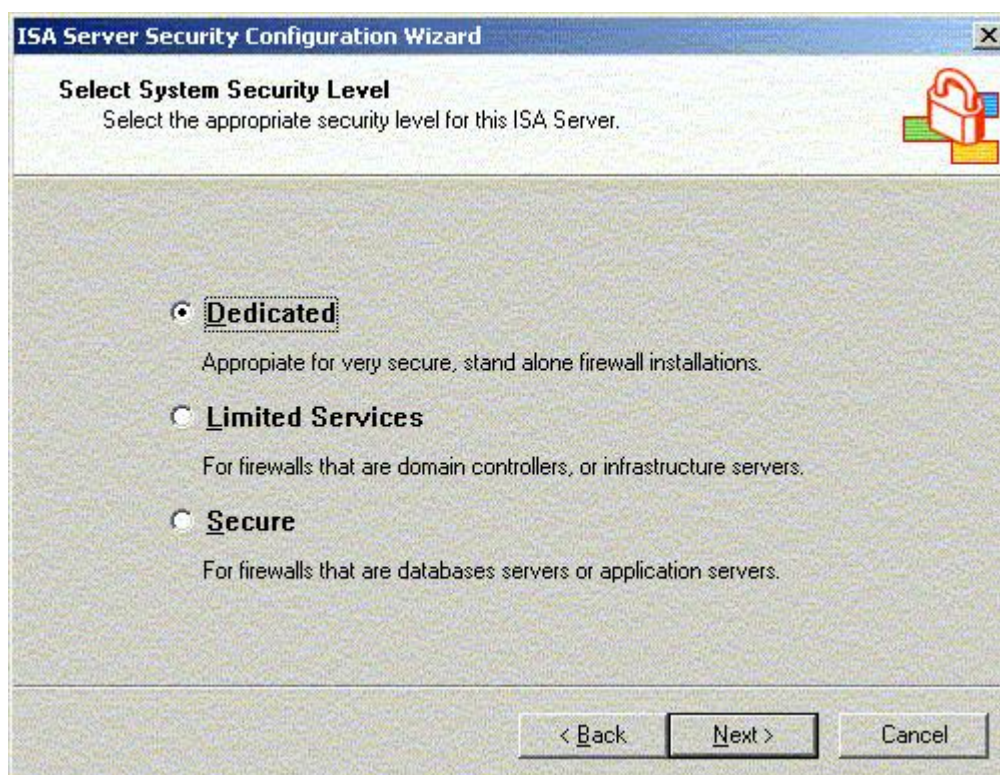
ISA Server Vulnerabilities

According to Sam Costello of IDG News Service,

"Microsoft Friday (08/17/01) said that one of its security products, Internet Security and Acceleration Server 2000, has three different security holes that could lead to denial of service attacks. Microsoft has issued a patch to fix all three vulnerabilities.

The flaws are unrelated and affect ISA Server's Voice-over-IP capabilities, its Proxy service and ISA's error page generation. The first vulnerability concerns a memory leak in the H.323 Gatekeeper service, which allows voice-over-IP traffic through a firewall. Each time malformed data is sent to this service, a small amount of the server's memory is depleted, Microsoft said. If such requests are sent frequently enough, the server would be slowed down to the point of disrupting normal use.

This problem is mitigated, however, in that the server can only be attacked if the H.323 Gatekeeper component is installed, something that only happens when a user chooses a "full installation," or to install everything on the software CD related to the application.

The second problem ISA Server faces is a denial-of-service problem in the software's Proxy service. This flaw, like the first, is also a memory leak that can cause a slowing of the server and lead to denial-of-service to legitimate users. This hole is made less serious because it can only be exploited by an internal user, Microsoft said.

Lastly, a complicated vulnerability in the way ISA Server handles error messages about irretrievable Web pages can allow an attacker to execute code and gain access to cookies on both the server and user machines. The flaw could be exploited if an attacker were able to trick a user into requesting a Web page that did not reside on a server. The false URL would also have to contain code. When ISA Server generates an error page stating that the requested page is not available, the code contained in the URL would run in the server's security domain and any cookies that server had set on the user's system would be available to the attacker. This vulnerability is limited in that the attacker would have to know which sites a user trusted, which sites had placed cookies on the user's computer and that the user had specific security settings that would allow the attack.

The H.323 Gatekeeper and Proxy Service flaws were discovered by Peter Grundl. The scripting hole was found by Hiromitsu Takagi.''[19]

We do not worry about the H.323 problem, as the corresponding service is not required in the GIAC network. Regarding the proxy flaws, the corresponding fixes are available from Microsoft. They must be applied to fix the above problems before the system can be used in the live network.

---

[19] http://www.nwfusion.com/news/2001/0817msisa.html

Default Port Assignments for Common Services

on a Windows 2000 Network

Since GIAC's network is mainly Windows based, it is essential to know the ports that might be involved in the network. The list below is provided by Microsoft at http://www.microsoft.com/windows2000/techinfo/reskit/en-us/default.asp?url=/WINDOWS2000/techinfo/reskit/en-us/cnet/cnfc_por_simw.asp :

Service Name	UDP	TCP
Browsing datagram responses of NetBIOS over TCP/IP	138	
Browsing requests of NetBIOS over TCP/IP	137	
Client/Server Communication		135
Common Internet File System (CIFS)	445	139, 445
Content Replication Service		560
Cybercash Administration		8001
Cybercash Coin Gateway		8002
Cybercash Credit Gateway		8000
DCOM (SCM uses udp/tcp to dynamically assign ports for DCOM)	135	135
DHCP client		67
DHCP server		68
DHCP Manager		135
DNS Administration		139
DNS client to server lookup (varies)	53	53
Exchange Server 5.0		
Client Server Communication		135
Exchange Administrator		135
IMAP		143
IMAP (SSL)		993
LDAP		389

LDAP (SSL)		636
MTA - X.400 over TCP/IP		102
POP3		110
POP3 (SSL)		995
RPC		135
SMTP		25
NNTP		119
NNTP (SSL)		563
File shares name lookup	137	
File shares session		139
FTP		21
FTP-data		20
HTTP		80
HTTP-Secure Sockets Layer (SSL)		443
Internet Information Services (IIS)		80
IMAP		143
IMAP (SSL)		993
IKE (For more information, see Table C.4)	500	
IPSec Authentication Header (AH) (For more information, see Table C.4)		
IPSec Encapsulation Security Payload (ESP) (For more information, see Table C.4)		
IRC		531
ISPMOD (SBS 2nd tier DNS registration wizard)		1234
Kerberos de-multiplexer		2053
Kerberos klogin		543
Kerberos kpasswd (v5)	464	464
Kerberos krb5	88	88
Kerberos kshell		544
L2TP	1701	
LDAP		389
LDAP (SSL)		636
Login Sequence	137, 138	139

Macintosh, File Services (AFP/IP)		548
Membership DPA		568
Membership MSN		569
Microsoft Chat client to server		6667
Microsoft Chat server to server		6665
Microsoft Message Queue Server	1801	1801
Microsoft Message Queue Server	3527	135, 2101
Microsoft Message Queue Server		2103, 2105
MTA - X.400 over TCP/IP		102
NetBT datagrams	138	
NetBT name lookups	137	
NetBT service sessions		139
NetLogon	138	
NetMeeting Audio Call Control		1731
NetMeeting H.323 call setup		1720
NetMeeting H.323 streaming RTP over UDP	Dynamic	
NetMeeting Internet Locator Server ILS		389
NetMeeting RTP audio stream	Dynamic	
NetMeeting T.120		1503
NetMeeting User Location Service		522
NetMeeting user location service ULS		522
Network Load Balancing	2504	
NNTP		119
NNTP (SSL)		563
Outlook (see for ports)		
Pass Through Verification	137, 138	139
POP3		110
POP3 (SSL)		995
PPTP control		1723
PPTP data (see Table C.4)		
Printer sharing name lookup	137	
Printer sharing session		139

Radius accounting (Routing and Remote Access)	1646 or 1813	
Radius authentication (Routing and Remote Access)	1645 or 1812	
Remote Install TFTP		69
RPC client fixed port session queries		1500
RPC client using a fixed port session replication		2500
RPC session ports		Dynamic
RPC user manager, service manager, port mapper		135
SCM used by DCOM	135	135
SMTP		25
SNMP	161	
SNMP Trap	162	
SQL Named Pipes encryption over other protocols name lookup	137	
SQL RPC encryption over other protocols name lookup	137	
SQL session		139
SQL session		1433
SQL session		1024 - 5000
SQL session mapper		135
SQL TCP client name lookup	53	53
Telnet		23
Terminal Server		3389
UNIX Printing		515
WINS Manager		135
WINS NetBios over TCP/IP name service	137	
WINS Proxy	137	
WINS Registration		137
WINS Replication		42
X400		102

PRIMARY Firewall Configuration Tutorial – Check Point FW-1

Configuring the Rulebase for FW1_B2C

Refer to the "Products Preparation" section for information on FW-1 and Windows NT hardening.

Security Policies:

FW1_B2C is the frontline firewall against outside intrusion along the B2C link. The security policy here contains the elements listed below (in the order specified below as well):

1. Ecommerce web service – TCP port 80 (HTTP) and 443 (SSL) allowed IN
2. Email service for the external world – TCP port 25 (SMTP) allowed IN
3. DNS service for the external world – UDP port 53 (DNS request) allowed IN
4. Drop and log everything else

Rule Processing and Orders:

FW-1 has a friendly yet powerful rulebase interface. As a security administrator, a centralized interface for defining all the security elements is good. However, FW-1 introduces confusions by allowing some of the security elements to be activated via separate properties dialogs. This is not only confusing, but is also giving room for conflicts. To truly determine the effective security policies, the combination of Security Policy Properties settings and RuleBase must be taken account into.

In FW-1, packets are matched in the following order:

1. Anti Spoofing
2. Properties marked FIRST in the Security Policy Properties
3. Rule base order except for the last rule

4.   Properties marked BEFORE LAST in the Security Policy Properties

5.   Rule Base last rule

6.   Properties marked LAST in the Security Policy Properties

7.   Implicit Drop Rule

One way to clear the confusion is to disable all the properties options and build every rule from scratch. Within the context of the rulebase, since FireWall-1 examines the Rule Base sequentially, rules must be carefully arranged in the appropriate order to prevent unwanted traffic from entering the network.

In GIAC's example here, the policy for Ecommerce, Email and DNS are not conflicting with each others, so the order between them does not matter. However, Rule 4 will deny everything, so it must be placed at the bottom, or nothing will be able to pass through the firewall.

In fact, placing the most frequently encountered rules at the top is good performance-wide. However, for a small and precise rulebase like the one we have here, it really does not matter.

There are certain special rules that are to be retained. These rules are:

- Stealth rule, which is positioned as the first rule in the rule base to prevent traffic from accessing the firewall itself directly.
- Implicit drop rule, which is added to the bottom of the Rule Base by default to drop all communication attempts not described by the other rules.

Rule Elements:

To define a rule in the FW-1 rulebase, the following components must first be defined:

- Source – the source network object(s)
- Destination – the destination network object(s)
- Service – the application protocol(s)
- Action – drop, accept, alert…etc
- Install On - the firewall itself

Network Objects:

Before we setup any rule, all the relevant network objects must be built first. The following issues must be considered:

■ The IDS is "invisible" to the outside world, and is not needed in this rulebase.

■ NAT is needed for the Ecommerce web server, the Email server and the DNS server.

■ FW-1 supports anti-spoofing by automatically generating rules that reject packets with internal IP addresses arriving on the external interface. For this feature to work, the Interfaces properties must be properly configured so that what is considered to be internal is clearly defined.

WWW

■ The Ecommerce web server

■ The server's address in the network is 192.168.8.3.

■ The server's "public" address for outside access is 192.168.7.8. This must be defined via the NAT tab. The corresponding NAT rules will be automatically generated.

■ Internal to the firewall

DNS

■ The DNS server

■ The server's address in the network is 192.168.8.4.

■ The server's "public" address for outside access is 192.168.7.9. This must be defined via the NAT tab. The corresponding NAT rules will be automatically generated.

■ Internal to the firewall
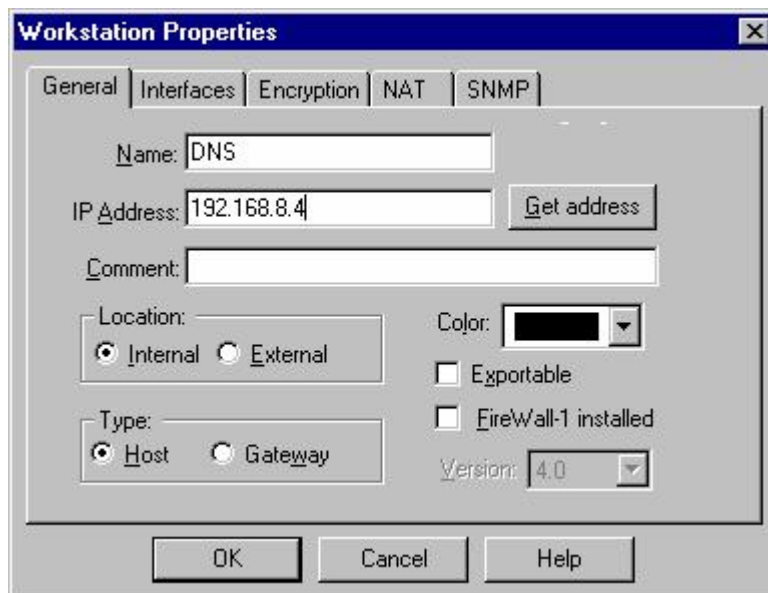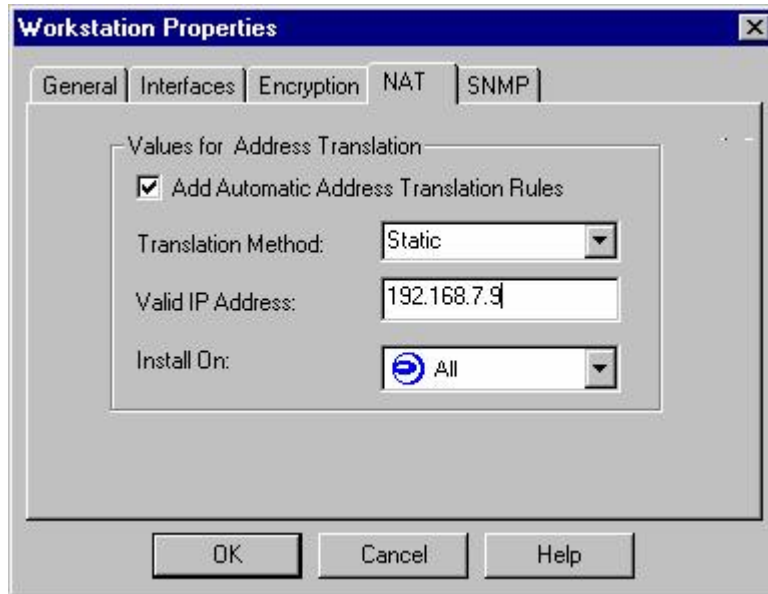
Email

- The SMTP server
- The server's address in the network is 192.168.8.5.
- The server's "public" address for outside access is 192.168.7.10. This must be defined via the NAT tab. The corresponding NAT rules will be automatically generated.
- Internal to the firewall
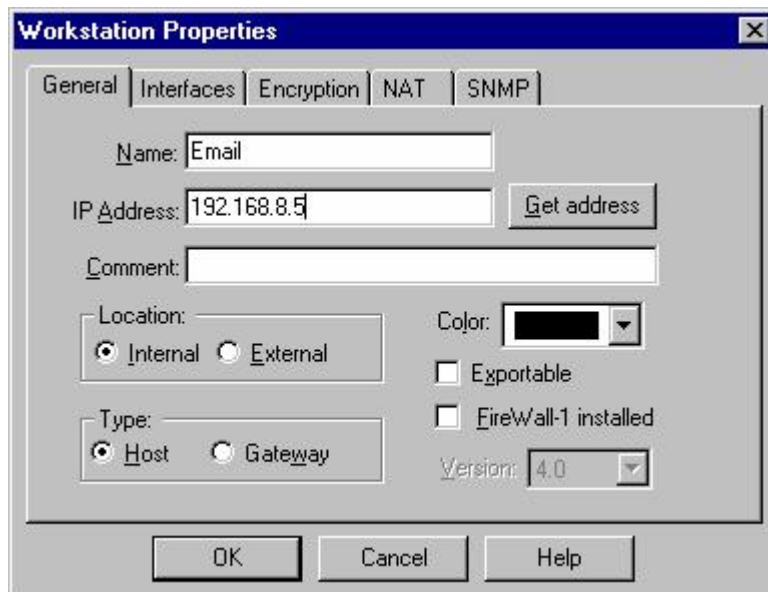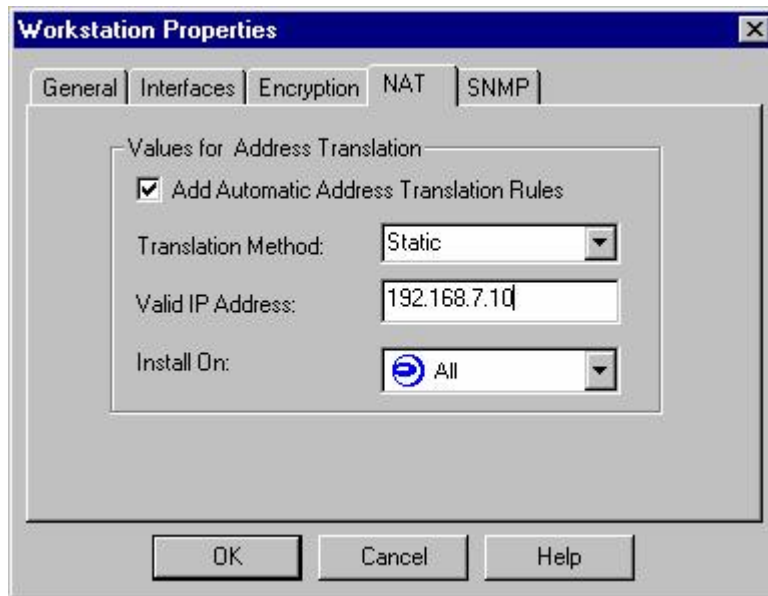
SELF

- FW1_B2C itself
- To the outside: 192.168.7.2
- To the inside: 192.168.8.2

Rules:

1,
Remove all the defaults (for security purpose) EXCEPT the "Accept Outgoing Packets" option. We need this for NAT to work (we have performed an experiment on this feature alone. Without this option, NAT fails).

Properties Setup

SYNDefender | LDAP | Encryption | Miscellaneous | Access Lists
Security Policy | Services | Log and Alert | Security Servers | Authentication

Apply Gateway Rules to Interface Direction: Inbound

TCP Session timeout: 3600   Seconds

☐ Accept FireWall-1 Control Connections

☐ Accept UDP Replies:

   Reply timeout: 40   Seconds

☑ Accept Outgoing Packets: Last

☐ Enable Decryption on Accept

☐ Accept RIP   First

☐ Accept Domain Name Queries (UDP)   First

☐ Accept Domain Name Download (TCP)   First

☐ Accept ICMP   Before Last

OK   Cancel   Help

The option "Apply Gateway Rules to Interface Direction" is related to the concept of interface direction, which specifies the communication direction in which a rule is enforced. With this option set to Inbound, security policy is enforced only on packets entering the object. With this option set to Outbound, policy is enforced only on packets leaving the object. With Eitherbound, policy is enforced both ways. We should stick with Inbound, as the overhead imposed by Eitherbound is too high.

2,

Enable the SynDefender Gateway to protect against potential Synflood attacks. A detailed description of the SynDefender options is available at http://www.phoneboy.com/faq/0137.html. In short, with the SynDefender Gateway option on, FireWall-1 will track the state of the handshaking process and will reset "invalid" connection attempts as necessary.
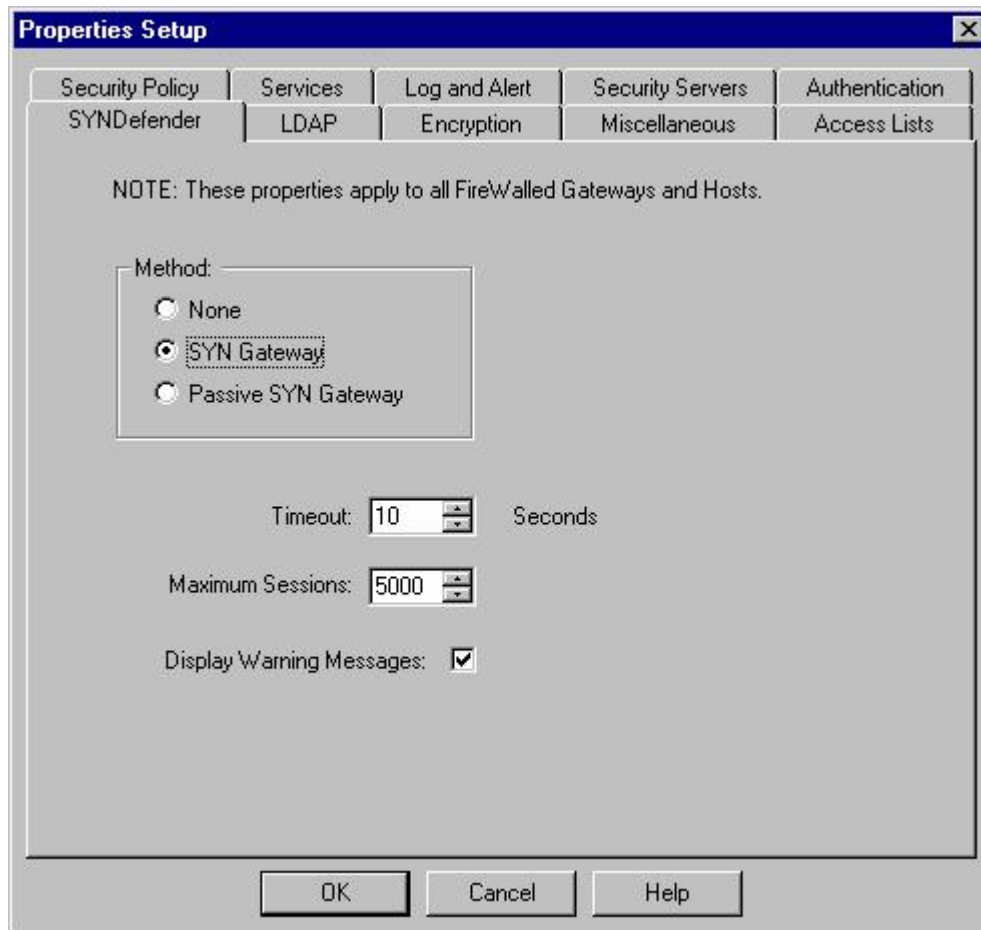
Keep in mind, SYN Gateway is resource intensive. It does produce negative performance impact. Therefore, the system running this service must be of reasonably high standard.

3,

Configure the following rules:

■ Allow only HTTP and HTTPS traffic to WWW.

■ Allow only DNS UDP traffic to DNS (DNS TCP traffic means zone transfer. We do not want that at all).

■ Allow only SMTP traffic to Email.

■ Drop everything else. Although by default everything gets dropped anyway, but an explicit drop will generate logs for the corresponding events, while an implicit drop will not. We want to log as much information as possible.

Any	WWW	http https	accept		Gateways	Any
Any	DNS	domain-udp	accept		Gateways	Any
Any	Email	smtp	accept		Gateways	Any
Any	Any	Any	drop		Gateways	Any

4,

Verify the rules. Click Policy – Verify to check and ensure that these rules are error free.
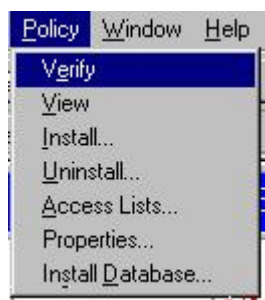
5,

Install the policy. Click Policy – Install. Install the policy on SELF (the firewall itself), which is the only policy enforcement point in this rulebase.

Install Security Policy Module

Install Security Policy on:

☑ SELF

Clear   All

OK   Cancel   Help
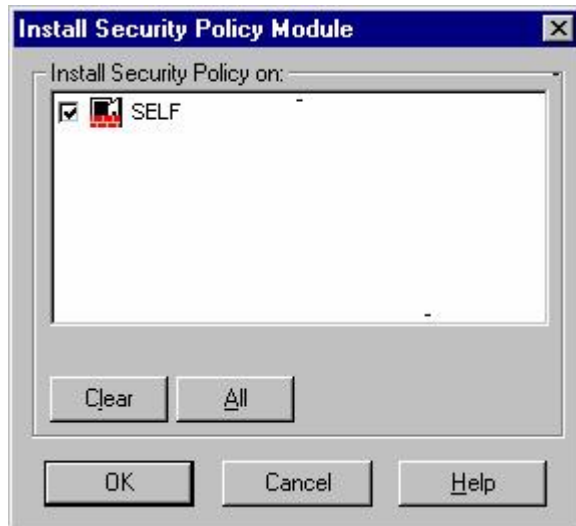
Standard.W: Security Policy Script generated into Standard.pf
Standard:
Compiled OK.

Installing Security Policy Standard on all.all@tsfw
Installing Security Policy on localhost(SELF) succeeded
Done.

If for some reasons the Policy was successfully verified but error occurs during installation, check the System Status and determine the health of the firewall.

Monitor - VPN-1 & FireWall-1 ...

File View Window Help

14Apr2002 18:18:18

SELF
Standard
🕐 14Apr2002 17:50:40
🛑 110
☑ 110
📝 1

For Help, press F1.   14Apr.
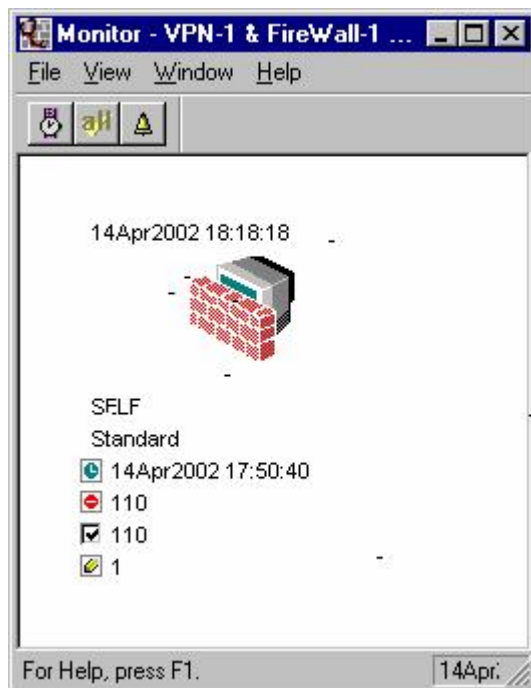
The possible statuses of the Firewall-1 Daemon are:

■ INSTALLED, meaning the daemon is running and that the security policy is installed

■ NOT INSTALLED, meaning the daemon is running, but then the security policy is not installed

■ DISCONNECTED, meaning there is no response from the daemon at all. Most likely the daemon has crashed.

6,

Configure routing. Since NAT occurs AFTER internal routing (and BEFORE transmission), we must manually set up the required persistent routes to ensure that NAT can be correctly performed.

For WWW, the command to use in NT's Command Prompt is:

route add –p 192.168.7.8 192.168.8.3

For DNS, the command to use in NT's Command Prompt is:

route add –p 192.168.7.9 192.168.8.4

For Email, the command to use in NT's Command Prompt is:

route add –p 192.168.7.10 192.168.8.5

The –p switch ensures that these entries can survive reboots by having them stored as persistent entries.

7,

Perform some basic testing:

To test the HTTP / HTTPS rule, do the following:

■ Deliberately set up telnet and FTP services to run on the WWW server. From the outside, connect to WWW via FTP and Telnet. The connection requests should fail.

■ From the outside, connect to WWW via HTTP and HTTPS. The connection requests should succeed.

To test the DNS query rule, do the following:

■ From the outside, use NSLOOKUP to initialize a zone transfer to DNS. The request should fail.

■ From the outside, use NSLOOKUP to simply query on DNS. The request should succeed.

■ Deliberately set up telnet and FTP services to run on DNS. From the outside, connect to DNS via FTP and Telnet. The connection requests should fail.

To test the Email rule, do the following:

■ Deliberately set up telnet and FTP services to run on Email. From the outside, connect to Email via FTP and Telnet. The connection requests should fail.

■ Send regular email messages to Email. The emails should arrive without problem.

Detailed testing and evaluation should be performed at the Audit stage.

8,

Open Log Viewer. View the log information and see if the log entries agree with the results obtained during the basic testing phrase. In our case, for sure they do.
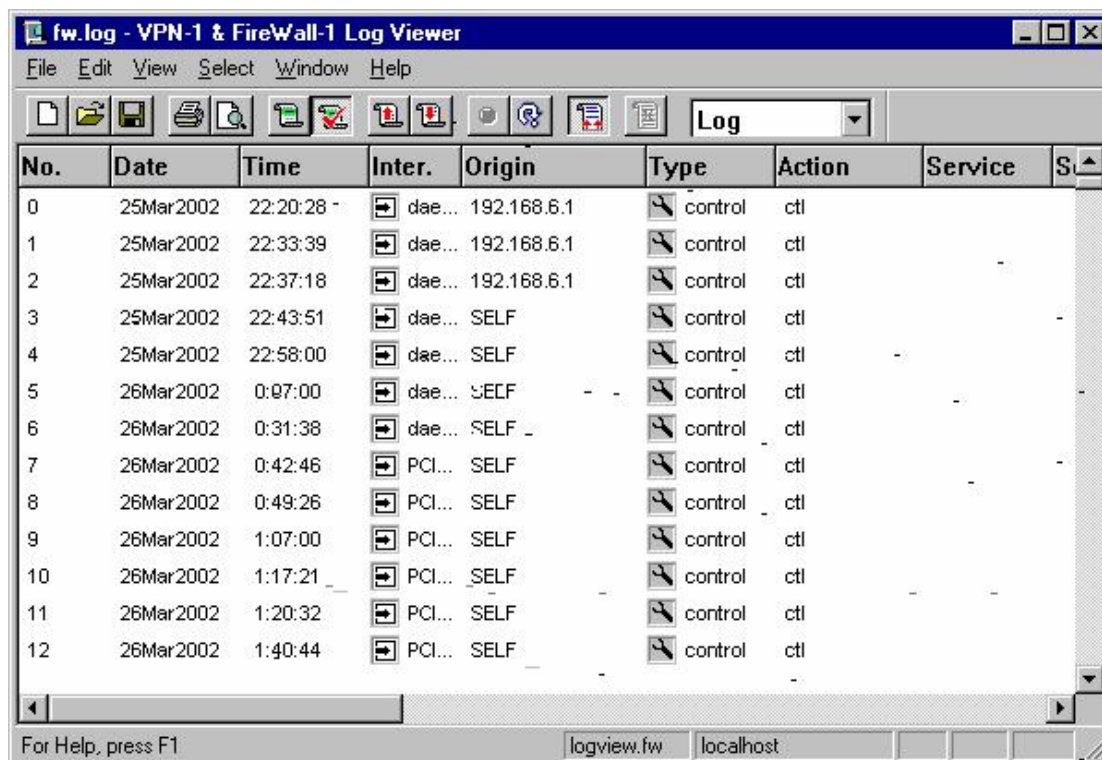
Note that there are 3 types of log: the Standard Log, the Accounting Log and the Active Log.
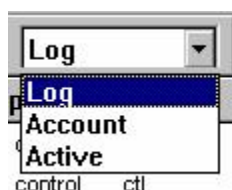
The Standard Log contains log entries of all events since the firewall service run. The Accounting Log holds entries for accounting and billing purpose, and is of no real use in our case. The Active Log shows the current connections that are going through the firewall. For our purpose, viewing the Standard Log and the Active Log is sufficient.
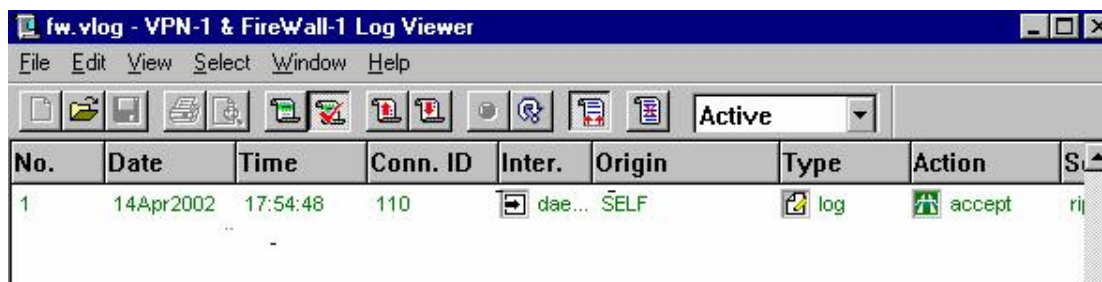
By default, the log includes too many columns. We can select the columns to view via the Select menu. We may then save the setting as a selection so that next time we can call up this same setting again.
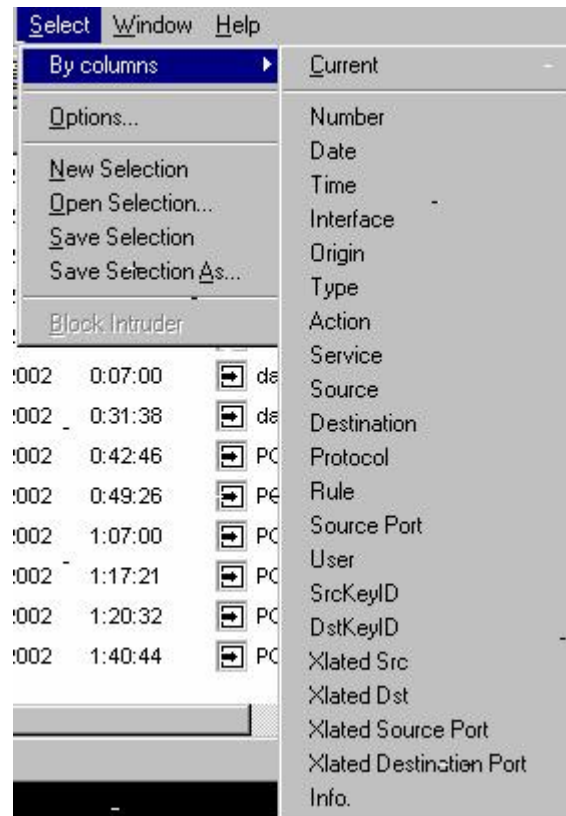
My recommendation for viewing logs on FW1_B2C – choose only the columns below:
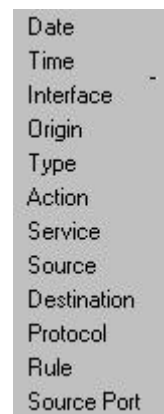
If the log file grows too big (this is possible in a busy network), consider to start a new log file. When a new log file is started, the current one will be automatically saved with a name that has the current date appended to it.

Apart from the log, we may, through the System Status interface, watch in real-time the number of packets that are Dropped, Rejected, Inspected and Logged.

Configuring the Rulebase for FW2_B2C:

Refer to the "Products Preparation" section on FW-1 and Windows NT hardening.

Security Policies and Orders:

FW2_B2C is the second layer of firewall protection against outside intrusion along the B2C link. It also prevents the internal staffs from tampering with the public service servers. The security policies here include:

1, Ecommerce web service:
- Any traffic allowed from Internal_Admin.
- HTTP/HTTPS traffic allowed from Internal_Dev (Developers use HTTP/HTTPS based update method such as Frontpage Server extension).
- HTTP/HTTPS traffic allowed from Internal_Clients.
- HTTP/HTTPS traffic allowed from RAS_Net.

2, External email service:
- Any traffic allowed from Internal_Admin.
- SMTP traffic allowed from the internal email server for retrieving and sending emails to and from the outside world.

3, External DNS service:
- Any traffic allowed from Internal_Admin.
- DNS query traffic allowed from Internal_Dev.
- DNS query traffic allowed from Internal_Clients.
- DNS query traffic allowed from RAS_Net.

4, IDS:

- The IDS can alert Internal_Admin via SMTP.
- Snort (http://www.snort.org/) is an ideal IDS software for such purpose.
- To be secure, the IDS itself is hardened and is protected by a firewall service running on itself.
- The IDS has its own SMTP service solely for sending alerts - sending emails to the administrator's mailbox located in the internal email server.

5, Drop and log everything else.

Since the above policies are not in conflicts, the order does not really matter as long as the "drop everything else" rule is the last rule. However, it is advised that the most frequently encountered rules be placed at the top. The web service, in the case of GIAC, is supposed to be the busiest one.

Network Objects:

Before we setup any rule, all the relevant network objects must be built first. Note that NAT is not needed on this configuration:

Admin
- The internal administrators network object
- The network address is 192.168.19.0
- Internal to the firewall

Dev
- The in-house developers network object
- The network address is 192.168.20.0
- Internal to the firewall

Staff
- The in-house clients network object
- The network address is 192.168.17.0
- Internal to the firewall

RAS_User
- The RAS users from the RAS_Net network object
- The network address is 192.168.22.0

- Internal to the firewall

WWW
- The Ecommerce web server
- The server's address in the network is 192.168.8.3.
- External to the firewall

DNS
- The DNS server
- The server's address in the network is 192.168.8.4.
- External to the firewall

Email
- The SMTP server
- The server's address in the network is 192.168.8.5.
- External to the firewall

IDS
- The IDS system
- The system's IP address is 192.168.8.6
- External to the firewall

Int_Email
- The internal email system
- For receiving IDS's email alert and subsequently retrieved by Internal_Admin internally
- The system's IP address is 192.168.18.4

SELF
- FW2_B2C itself
- To the outside: 192.168.8.1
- To the inside: 192.168.16.1

Rules and Orders:

1,
Remove all the defaults EXCEPT the "Accept Outgoing Packets" option.

2,

Do not enable the SynDefender Gateway option. It is not likely to see Synflood attacks against this firewall from the inside network.

3,

Configure the following rules:

- Allow Admin access to all servers in Public_Services via any traffic.
- Allow Staff access to WWW via HTTP and HTTPS.
- Allow Staff access to DNS via DNS query.
- Allow Dev access to WWW via HTTP and HTTPS.
- Allow Dev access to DNS via DNS query.
- Allow RAS_User access to WWW via HTTP and HTTPS.
- Allow RAS_User access to DNS via DNS query.
- Allow Int_Email to receive SMTP alerts from IDS. We need this rule so that the alerts can be forwarded to the administrator's mail box. Keep in mind though, that with this rule in place, the IDS must be absolutely secure, or an intrusion path to the inside network will come true.
- Allow Int_Email to initiate SMTP requests to Email. We need this rule so that the internal email system can initialize communication with the external one for sending outbound emails and retrieving inbound queued emails

4,

Drop and log everything else. This rule must be the LAST rule.

Except for the last "Drop everything rule", the order of the rules we defined does not matter given the small number of rules and their non-conflicting nature.

5,

Verify the policy via Policy – Verify.

6,

Install the policy via Policy – Install. Install the policy onto SELF.

7,

Perform some basic testing.

8,

Review the log via the Log Viewer.

Basic Testing:

- From Internal_Clients, use NSLOOKUP to initiate a DNS zone transfer to the DNS server. The zone transfer attempt should fail.
- Deliberately create a share on the WWW server, then try to map to this share from Internal_Dev. The mapping attempt should fail.
- Deliberately enable FTP on the WWW server, then try to FTP to it from Internal_Clients. The FTP attempt should fail.
- Trigger an intrusion on the IDS. See if the administrator can be alerted.
- Inspect the log file.

In-depth testing should be conducted at the Audit stage.

Configuring the Other Devices

Configuring the Norton1_IDS Firewall:

Refer to the "Products Preparation" section for information on Norton Personal Firewall 2002.
Refer to the "Products Preparation" section for information on Windows 2000 hardening.

Norton1_IDS sits between the internal core switch and the Internal_Clients segment.

Security Policy:

The policies to be enforced here are:

1. No connection towards Internal_Clients can ever be initiated from any other segment (except from Internal_Admin).
2. Outbound access requests made by Internal_Clients are not restricted by this firewall, but by other firewalls on the network.
3. When the clients access the internet, Java and ActiveX codes are blocked.
4. Drop and log everything else.

The configuration of Norton Firewall 2002 requires emphasis on the concept of trusted zones and security levels. There is no sophisticated mechanism for defining individual rules. The good thing about this approach is the simplicity of configuration and administration. The drawback is the lack of flexibility and precise control. Therefore, this firewall is only used at the departmental level for protecting users, not services.

Defining the Zones:

To properly configure the Norton Firewall at this location, the key is to define the Trusted Zones and the Restricted Zones. Trusted Zones can enjoy almost all sorts of access, and are typically the internal network segments. Restricted Zones, on the other hand, are the external networks that are not to be trusted. Connections cannot be initiated from these zones to pass through the firewall.

■ In our network, Internal_Clients (192.168.17.0) can freely access Internal_Servers (192.168.18.0). Whether or not traffic can be initiated from Internal_Servers depends on the server applications in use. Since Internal_Servers is pretty secure, and just in case that certain maintenance traffic has to originate from the servers to the clients, we will have both 192.168.18.0 and 192.168.17.0 configured as Trusted.

■ Since Internal_Clients is trusted, in theory it can make outgoing internet access requests to everywhere. We will, however, implement internet access restrictions on an as-needed basis at ISA_Cache.

■ Internal_Admin (192.168.19.0) can access Internal_Clients and not vice versa, meaning 192.168.19.0 should be treated as Trusted. We will block Internal_Clients's requests towards Internal_Admin via Norton2_IDS.

■ Critical_Resources (192.168.21.0) can be accessed by Internal_Clients and not vice versa, so 192.168.21.0 should be Restricted. No direct access from Public_Services (192.168.8.0) is ever allowed, so 192.168.8.0 should be Restricted as well. Internal_Clients's requests towards Public_Services are further filtered at FW2_B2C.

■ No requests towards Internal_Clients can be made from RAS_Net (192.168.22.0) Core_Net (192.168.16.0) nor Internal_Dev (192.168.20.0). These subnets should be Restricted altogether.

Configure the Security Level:

We need the highest possible level of security here. To set such security, use Custom Settings, and set everything to High. All the alert options should be enabled as well.
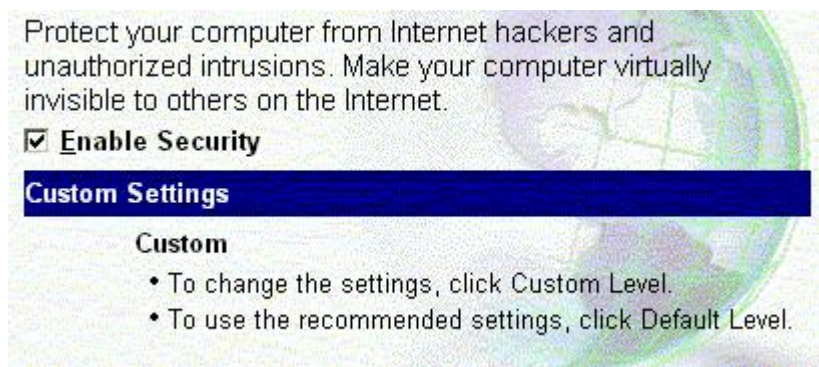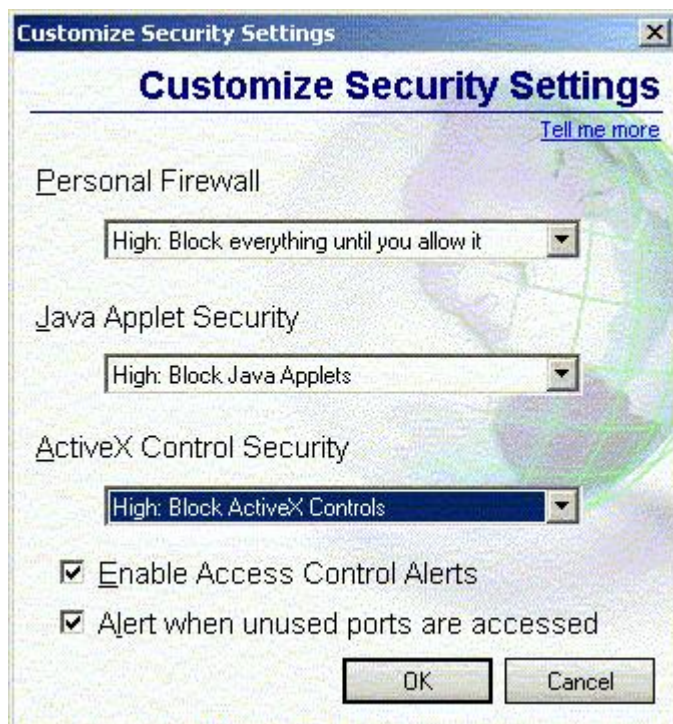
Configure the Advanced Options:

In the Advanced Options section, enable the following options:

- Block IGMP Protocol: IP multicast is not to be used in our network anyway.
- Stealth Blocked Ports: This causes the blocked ports to not respond to enquiries from the outside. Such option eliminates the hacker's opportunity of learning any unnecessary network information.
- Block Fragmented IP Packets: Fragmented IP packets are often used as a way to attack systems. This option protects against such threat.
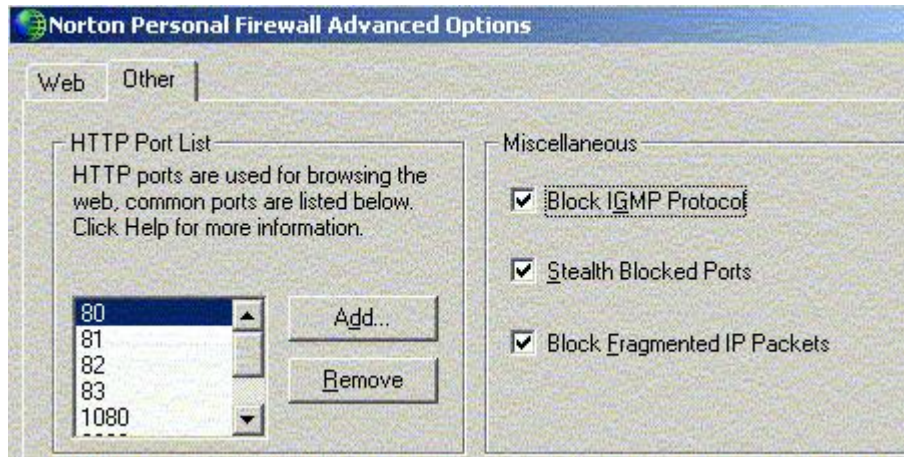
Configure Intrusion Detection:

Norton Firewall can detect port scan attempts and automatically block the attackers from making further connection attempts. We should take advantages of these functionalities.
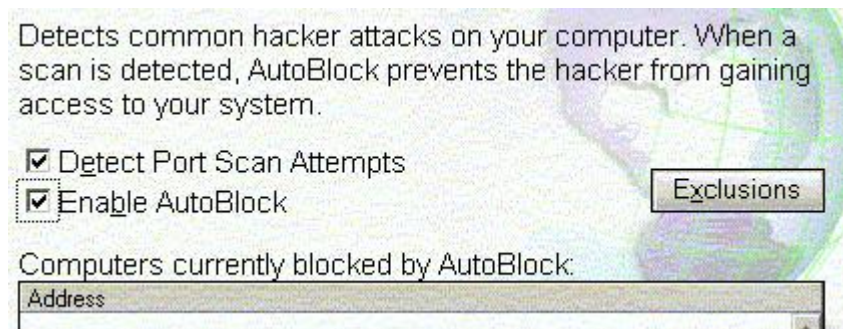
Configure Logging:

We should always opt for logging as much information as possible. Set the Reporting Level to High and ensure that your drive is large enough to hold the large amount of logged data.

Drag the slider to set the Reporting Level

High
- Provides the most information about Internet security events.
- Notifies you of blocked Web site content, security alerts, and applications accessing the Internet.
- Appropriate if you want to keep a careful watch on all activity.

Basic Testing:

■ From Internal_Clients, access a file share in Internal_Servers. The request should succeed.

■ From Internal_Clients, access an internet web site via ISA_Cache's port 8080. The request should succeed.

■ From RAS_Net, access a file share in Internal_Clients. The request should fail.

■ Inspect the log file.

Further in-depth testing should be conducted at the Audit stage.

Configuring the Norton2_IDS Firewall:

Refer to the "Products Preparation" section for information on Norton Personal Firewall 2002.

Refer to the "Products Preparation" section for information on Windows 2000 hardening.

Norton2_IDS sits between the internal core switch and the Internal_Admin segment.

Security Policy:

The policies to be enforced here are:

1. No connection towards Internal_Admin can ever be initiated from any other segment.
2. Outbound access requests made by Internal_Admin are not restricted by this firewall.
3. When the administrators access the internet, Java and ActiveX codes are blocked.
4. Drop and log everything else.

Defining the Zones:

■ In our network, Internal_Admin (192.168.19.0) can access anywhere. Therefore, 192.168.19.0 must be Trusted.

■ No requests towards Internal_Admin can ever be made from Internal_Clients (192.168.17.0), Internal_Dev (192.168.20.0), Critical_Resources (192.168.21.0), Public_Services (192.168.8.0), RAS_Net (192.168.22.0) nor Core_Net (192.168.16.0). These subnets should all be Restricted.

■ Whether or not traffic can be initiated from Internal_Servers depends on the server applications in use. Since Internal_Servers is pretty secure under the protection of the VisNetic firewall, and just in case that certain maintenance traffic has to originate from the servers to the clients, we will have Internal_Servers (192.168.18.0) configured as Trusted.

Configure the Security Level:

We need the highest possible level of security here. To set such security, use Custom Settings, and set every blocking option to High. All the alert options should be enabled as well.

Configure the Advanced Options:

In the Advanced Options section, enable the following options:

■ Block IGMP Protocol: IP multicast is not to be used in our network anyway, so this option should be blocked.
■ Stealth Blocked Ports: This causes the blocked ports to not respond to enquiries from the outside. Such option eliminates the hacker's opportunity of learning any unnecessary network information.
■ Block Fragmented IP Packets: Fragmented IP packets are often used as a way to attack systems. This option disables such threat.

Configure Intrusion Detection:

Norton Firewall can detect port scan attempts and automatically block the attackers from making further connection attempts. Enable all of these features.

Configure Logging:

We should always opt for logging as much information as possible. Set the Reporting Level to High and ensure that your drive is large enough to hold the large amount of logged data.

Basic Testing:

■ From Internal_Admin, access a file share in Internal_Servers. The request should succeed.
■ From Internal_Admin, access an internet web site via ISA_Cache's port 8080. The request should succeed.
■ From RAS_Net, access a file share in Internal_Admin. The request should fail.
■ Inspect the log file.

Further in-depth testing should be conducted at the Audit stage.

Configuring the Norton3_IDS Firewall:

Refer to the "Products Preparation" section for information on Norton Personal Firewall 2002.
Refer to the "Products Preparation" section for information on Windows 2000 hardening.

Norton3_IDS sits between the internal core switch and the Internal_Dev segment.

Security Policy:

The policies to be enforced here are:

1. No connection towards Internal_Dev can ever be initiated from any other segment.
2. Outbound access requests made by Internal_Dev are not restricted by this firewall, but by other firewalls on the network.
3. When the developers access the internet, Java and ActiveX codes are blocked.
4. Drop and log everything else.

Defining the Zones:

■ In our network, Internal_Dev (192.168.20.0) itself must be trusted so that it can make outgoing requests. Its requests towards the internet should be restricted at ISA_Cache. Its requests towards Public_Services should be filtered at FW2_B2C.

■ For network maintenance and other administrative purposes, Internal_Admin (192.168.19.0) must be allowed to access Internal_Dev. Therefore, 192.168.19.0 should be in the Trusted list.

■ No requests towards Internal_Dev can ever be made from Internal_Clients (192.168.17.0), Critical_Resources (192.168.21.0), Public_Services (192.168.8.0), RAS_Net (192.168.22.0) nor Core_Net (192.168.16.0). These subnets should all be Restricted.

■ Whether or not traffic can be initiated from Internal_Servers depends on the server applications in use. Since Internal_Servers is pretty secure under the protection of the VisNetic firewall, and just in case that certain maintenance traffic has to originate from the servers to the clients, we will have

Internal_Servers (192.168.18.0) configured as Trusted.

Configure the Security Level:

We need the highest possible level of security here. To set such security, use Custom Settings, and set every blocking option to High. All the alert options should be enabled as well.

Configure the Advanced Options:

In the Advanced Options section, enable the following options:

- Block IGMP Protocol: IP multicast is not to be used in our network anyway, so this option should be blocked.
- Stealth Blocked Ports: This causes the blocked ports to not respond to enquiries from the outside. Such option eliminates the hacker's opportunity of learning any unnecessary network information.
- Block Fragmented IP Packets: Fragmented IP packets are often used as a way to attack systems. This option disables such threat.

Configure Intrusion Detection:

Norton Firewall can detect port scan attempts and automatically block the attackers from making further connection attempts.

Configure Logging:

We should always opt for logging as much information as possible. Set the Reporting Level to High and ensure that your drive is large enough to hold the large amount of logged data.

Basic Testing:

- From Internal_Dev, access a file share in Internal_Servers. The request should succeed.
- From Internal_Dev, access an internet web site via ISA_Cache's port 8080. The

request should succeed.

■ From RAS_Net, access a file share in Internal_Dev. The request should fail.

■ Inspect the log file.

Further in-depth testing should be conducted at the Audit stage.

Configuring the VisNetic_1 Firewall:

Refer to the "Products Preparation" section for information on VisNetic Firewall.

Refer to the "Products Preparation" section for information on Windows 2000 hardening.

VisNetic_1 sits between the core switch and the following segments:

- 192.168.18.0 (Internal_Servers)
- 192.168.21.0 (Critical_Resources)
- 192.168.22.0 (RAS_Net)

Security Policies and Orders:

The policies to be enforced here are:

1. Only Internal_Admin can freely access all segments behind this firewall with any protocol he/she likes.
2. External partners and suppliers can access only the Critical_Resources segment. Such access must originate from Core_Net via W2K_VPN, using HTTP and HTTPS as the protocols. Their access must be restricted by application level authentication and authorization.
3. Internal_Clients and Internal_Dev can access Internal_Servers with any protocol, although their access must be restricted by system level authentication and authorization.
4. Internal_Clients and Internal_Dev can access Critical_Resources only via HTTP and HTTPS. Their access must be restricted by application level authentication and authorization.
5. RAS users who connect via RAS_Net can access the Internal_Servers segment with any protocol, although their access must be restricted by system level authentication and authorization. Their access to Public_Services is subject to filtering at FW2_B2C.
6. Drop and log everything else.

Since the rulebase for VisNetic is effective on a per-interface basis, order of rules is relevant only within the context of individual interface. Rules within each interface are processed sequentially, which is exactly the same as the way rules are processed in

FW-1.

We cannot rely solely on the firewall to provide all sorts of protections!!!

I have allowed Internal_Clients, Internal_Dev and RAS_Net users access to Internal_Servers with whatever protocols they like. The rationales are:

- *There are so many different types of services possible in a Microsoft Windows based Network, that many of these services rely on multiple protocols that are mutually dependent. Blocking these protocols one by one is possible, but is imposing heavy administrative burden, especially when new applications using new protocols are regularly introduced (given the pace of technological advance, this is highly likely possible).*
- *Different users in the Internal_Clients group requires access to different services. Blocking at the firewall can be inflexible and troublesome.*

Therefore it is recommended that, for Internal_Servers, access be restricted through the use of system level ACL and application level authentication, rather than through firewall filtering.

Defining the Interfaces:

VisNetic has its rules configured on a per-interface basis. So, for traffic to pass through it and obtain a feedback from the other side, configuration must be made on all the interfaces involved.

VisNetic_1 has the following interfaces:

- 192.168.16.6 (to the core switch / Core_Net)
- 192.168.18.1 (to Internal_Servers)
- 192.168.21.1 (to Critical_Resources)
- 192.168.22.1 (to RAS_Net)

The Configuration Wizard can be used to put the idle interfaces to an "unused" state.

An Interface Configuration Example:

As mentioned before, VisNetic has its rules configured on a per-interface basis. FOR EXAMPLE, if a rule is needed to allow HTTP access from the clients in 192.168.16.0 to the intranet web server in 192.168.18.0, the following interface configurations must be made:

1,
Configure the interface attached to 192.168.18.0 to accept all traffics. 192.168.18.0 is considered as a trusted local network to the firewall (while the 192.168.16.0 network is considered as untrusted and remote).

2,
Configure the interface attached to 192.168.16.0 to filter all traffics. By doing so, all traffic will be blocked by this interface UNLESS rules are configured to allow exceptions.
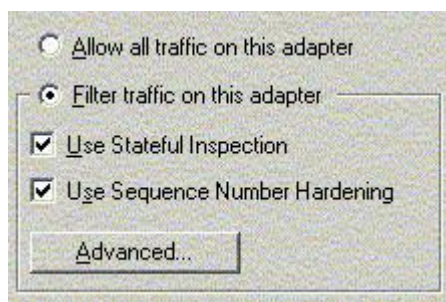
3,
Add a new rule to allow HTTP access. This involves the TCP protocol with a "In & Out" nature:

- ■ "In" defines traffic from Remote to Local
- ■ "Out" defines traffic from Local to Remote
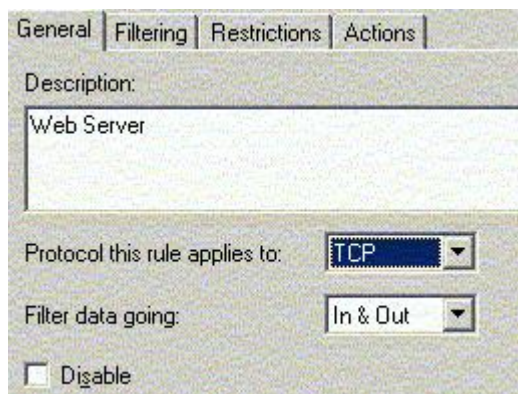
In the Filtering section, define the address ranges of the parties involved in the access. The intranet web server network is on the local side. It listens on port 80. On the other hand, a HTTP client uses a port above 1023 to initiate request from the remote side.
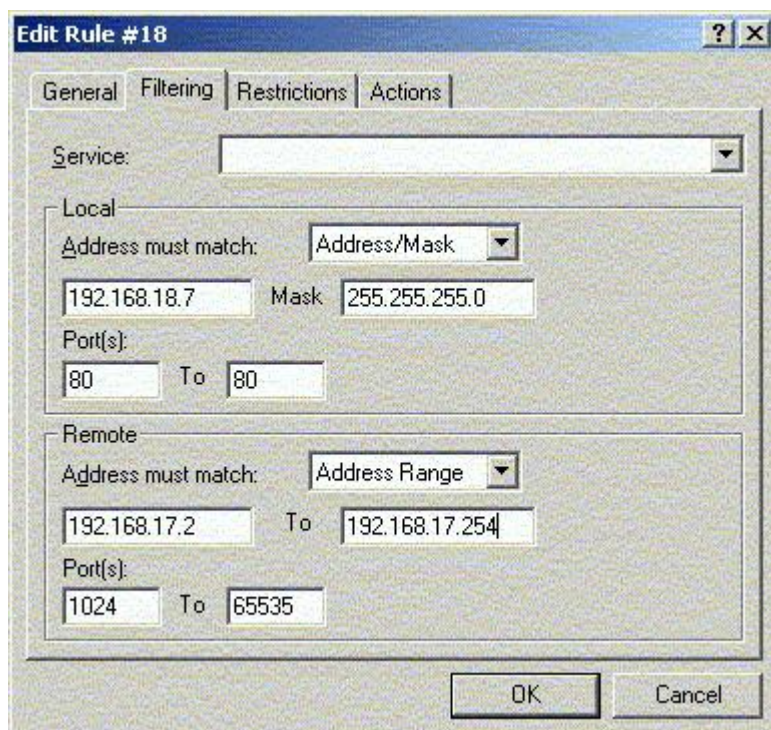
Fragments should be blocked, and rules should be effective all the time. However, do NOT enable "Block incoming connections", or any connection attempt will fail.
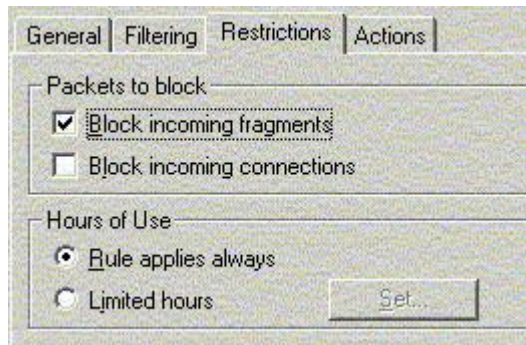
Set the action to "Allow" for this rule, and configure the firewall to log all the items.
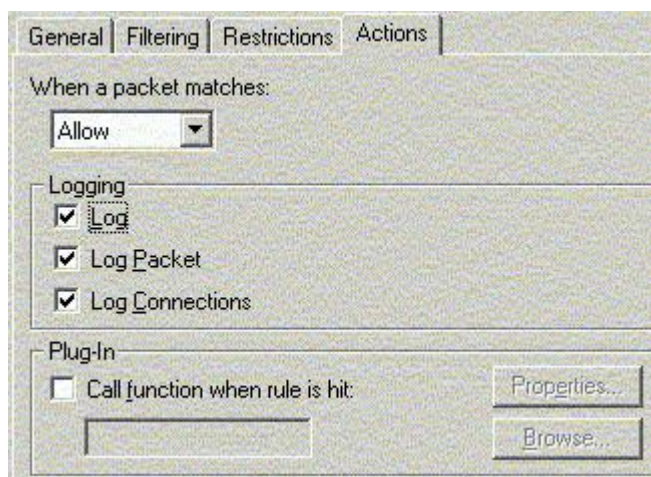
Finally, double check and ensure that ARP is fully allowed both in and out. In fact, as long as traffic transaction is involved with an interface, ARP should be fully allowed in both directions.

Save the rules. Unlike Check Point FW-1, there is no need to reinstall the policy every time a change is made.

Local Interface Configuration:

At VisNetic_1, we are trying to protect the following trusted subnets:

- Internal_Servers (192.168.18.0)
- Critical_Resources (192.168.21.0)

These subnets are to be treated as local by the respective interfaces of VisNetic_1:

- 192.168.18.0 – trusted by 192.168.18.1
- 192.168.21.0 – trusted by 192.168.21.1

Thus, interface 192.168.18.1 and 192.168.21.1 should be configured to allow all traffic. On the other hand, RAS_Net (192.168.22.0) includes dial-in users, and is considered as remote and untrusted.

External Interface Configuration:

Now, we need to determine the remote subnets that need to access the trusted subnets listed in the last section. One obvious external interface on VisNetic_1 is 192.168.16.6, which is the Core_Net connected to the core switch. On this interface traffic must be filtered, with rules being configured as follow (segment on the left represents the local side, while the one on the right represents the remote side):

- Internal_Servers (192.168.18.0) <- IN & OUT, Microsoft Networking, DNS Query, SMTP, POP3, HTTP, FTP -> Internal_Clients (192.168.17.0)
- Internal_Servers (192.168.18.0) <- IN & OUT, Microsoft Networking, DNS Query, SMTP, POP3, HTTP, FTP -> Internal_Dev (192.168.20.0)
- Critical_Resources (192.168.21.0) <- IN & OUT, HTTP and HTTPS -> Internal_Clients (192.168.17.0)
- Critical_Resources (192.168.21.0) <- IN & OUT, HTTP and HTTPS -> Internal_Dev (192.168.17.0)
- Critical_Resources (192.168.21.0) <- IN & OUT, HTTP and HTTPS -> Core_Net VPN Clients (Address range: 192.168.16.55 to 192.168.16.65)
- Any <- IN & OUT, Any -> Internal_Admin (192.168.19.0)

- DISALLOW Any <- IN & OUT, Any -> Any

Another interface which requires filters to be setup is the interface attached to RAS_Net, which is 192.168.22.1:

- RAS_Net (192.168.22.0) <- IN & OUT, Any -> Internal_Servers (192.168.18.0)
- RAS_Net (192.168.22.0) <- IN & OUT, HTTP, HTTPS and DNS Query -> Public_Services (192.168.8.0)
- DISALLOW Any <- IN & OUT, Any -> Any

Depending on the needs of the users, additional traffic may be allowed. Refer to the "Products Preparation" section for a full list of protocols commonly used in a Windows based network.

It is always a good practice to explicitly add a "drop everything" rule as the last rule. This ensures that all illegitimate requests are logged.

Basic Testing:

- From an internal client, access a share that belongs to the file server inside Internal_Servers. The attempt should succeed.
- From an internal client, access the database application server inside Critical_Resources via telnet. The attempt should fail.
- From an invalid internal client, access the intranet server inside Internal_Servers via HTTP. The attempt should fail.
- Inspect the log file.

Further testing should be performed at the Audit stage.

Configuring the Proxy Server

Refer to the "Products Preparation" section for information on Microsoft ISA Server.
Refer to the "Products Preparation" section for information on Windows 2000 hardening.

This section focuses on the configuration of ISA Server's Proxy functions. In fact, ISA Server's role in terms of firewalling in this project is simple and straight forward: Drop ALL incoming requests made from the internet!

The internal staffs at GIAC need to access the internet frequently. It is not economical nor scalable if true IP is implemented for each client. On the other hand, simple NAT does not produce any performance benefit. Thus, a proxy server that combines NAT and caching should be implemented.

A proxy server is a server that sits between a client application and a real server that intercepts all requests to the real server to see if it can fulfill the requests itself. As described by Webopedia.com, proxy servers have two main purposes:

"Improve Performance: Proxy servers can dramatically improve performance for groups of users. This is because it saves the results of all requests for a certain amount of time. Consider the case where both user X and user Y access the World Wide Web through a proxy server. First user X requests a certain Web page, which we'll call Page 1. Sometime later, user Y requests the same page. Instead of forwarding the request to the Web server where Page 1 resides, which can be a time-consuming operation, the proxy server simply returns the Page 1 that it already fetched for user X. Since the proxy server is often on the same network as the user, this is a much faster operation. Real proxy servers support hundreds or thousands of users. The major online services such as Compuserve and America Online, for example, employ an array of proxy servers.

Filter Requests: Proxy servers can also be used to filter requests. For example, a company might use a proxy server to prevent its employees from accessing a specific set of Web sites."[20]

---

[20] http://www.webopedia.com/TERM/P/proxy_server.html

Security Policy:

1. Provide proxy service for internal clients accessing the internet. Protocols allowed include: HTTP, HTTPS, FTP, SMTP, POP3, IMAP, DNS, NNTP
2. Provide HTTP and FTP caching service for internal clients accessing the internet.
3. Allow outgoing PPTP traffic from internal PPP based VPN clients accessing external partners' VPN sites.
4. Prevent unauthorized users from accessing the proxy service.
5. Disallow any incoming requests from the outside world.
6. Disallow everything else.

Rulebase Confusion

ISA Server supports dynamic filtering, meaning ports are opened and closed on an on-demand basis. At the same time, ISA Server supports packet filtering, which is static in nature. So, what is the difference? Somehow most ISA Server documentations out there fail to clearly explain the difference.

In fact, ISA Server provides security via the following means:

■ Access Policy -> Protocol Rules - allow internal client access to the Internet. This is dynamic in nature.
■ Access Policy -> Packet filtering rules – open or close port statically.
■ Publishing Rules - allow external clients access to internal servers. This is dynamic in nature as well.

In the case of GIAC, we can control outgoing requests using access policy or protocol rules. We do not need to use any publishing rule, as there is no service under the protection of this ISA Server. To prevent external access through this ISA Server, we should statically block all access attempts made from the outside.

ISA Server Configuration:

ISA_Cache is a Microsoft ISA server based caching solution. It sits between the internal core switch and Router_Eiconcard. The reason why Microsoft ISA Server is deployed is because it combines the features of stateful inspection based firewall technologies and advanced caching mechanism, making it a secure performer.

When installation is completed, run the Getting Started Wizard. Below are the configuration options that deserve special attentions.

Basic Caching Options:

First of all, the default cache size of 100MB may not be enough. The factors to consider include the number of users and the frequency of use. Since hard drive space is cheap anyway, we should make the size much larger than this, say 500MB.
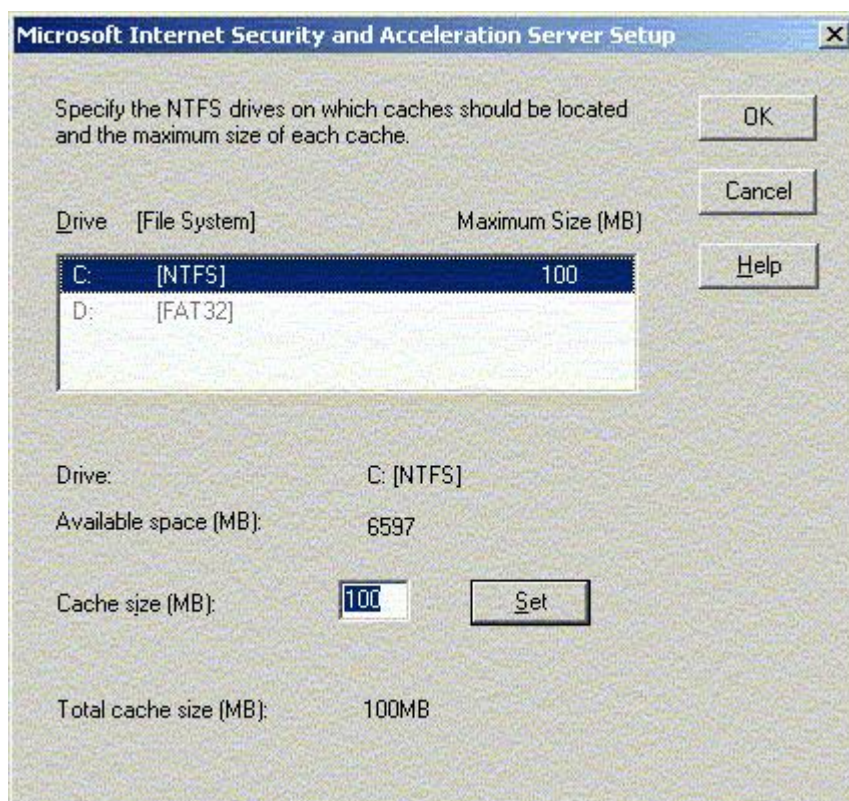
All of our internal subnets, especially those that contains users (Internal_Clients,

Internal_Admin, Internal_Dev), should be configured as "internal". Press the Construct Table button to allow ISA Server to build a table for address mapping. These addresses should be tied to the internal interface of ISA_Cache, which is 192.168.16.7.

Keep in mind, the construction of this LAT (Local Address table) is very important, as ISA Server relies solely on it to distinguish between trusted nodes and untrusted nodes. If there are changes to the IP address settings, this LAT must be reconstructed. And since the construction of LAT relies heavily on information provided by the routing table, you must ensure that there is no invalid routing entry. Using automatic mechanism like RIP eliminates the need for manually changing the routing table.
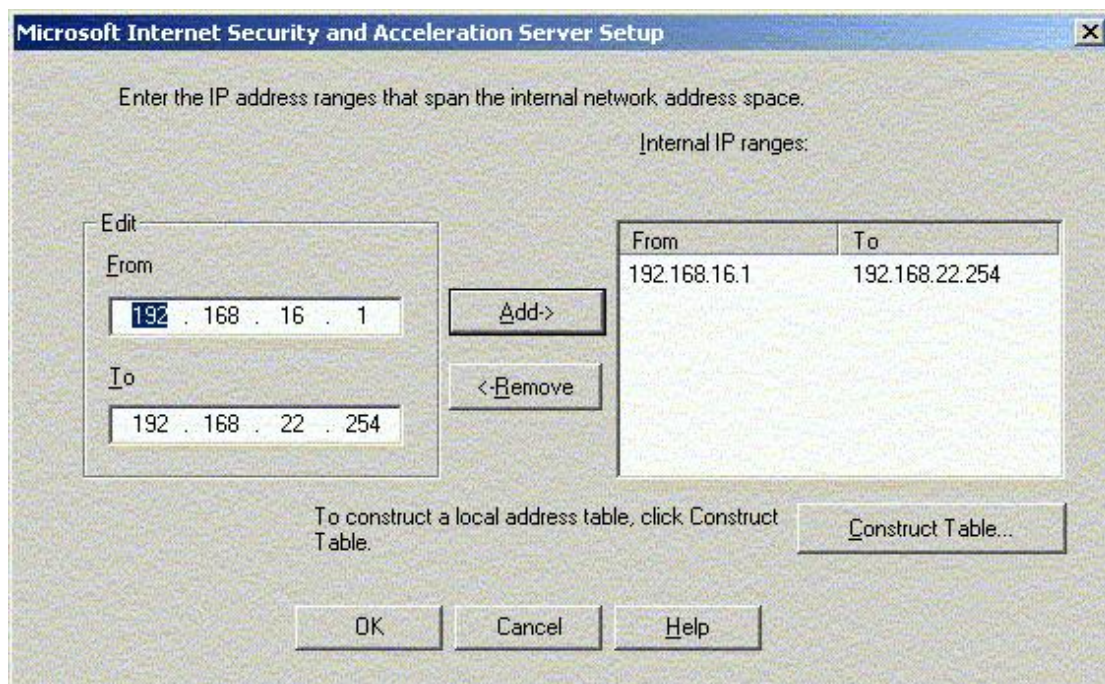
Only include the local interface in the LAT. Do not include the internet interface, or ISA will mis-behave.
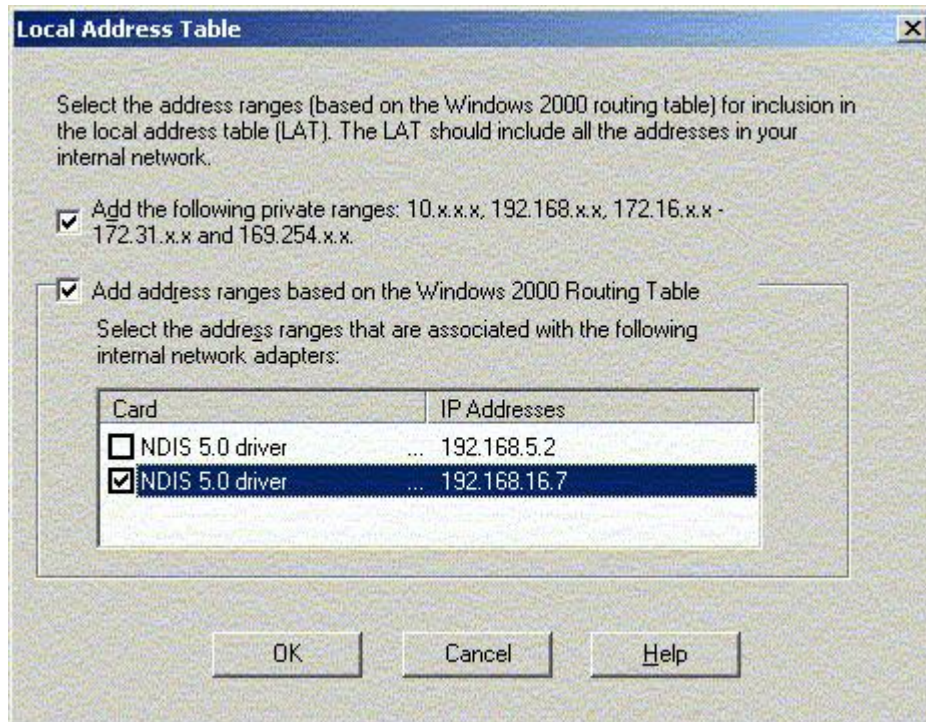
The internal clients should be properly defined as client sets. These clients include all users that need to access the internet, meaning the staffs, the administrators, the developers and the servers. Each of them should be presented by an individual client set.

Protocol Rules:

Protocol rules in ISA Server determine which protocols clients can use to access the internet. The protocols that the users use must be carefully selected. Rules are applied to allow outbound requests only on these protocols.

These protocols are application specific. For example, AOL Messenger and ICQ use different protocols. Whether or not these applications are allowed is a matter of company policy, and is out of the scope of this project. To be certain, the following protocols are almost always needed:

■ HTTP
■ HTTPS
■ FTP
■ SMTP
■ POP3
■ IMAP

- DNS
- NNTP
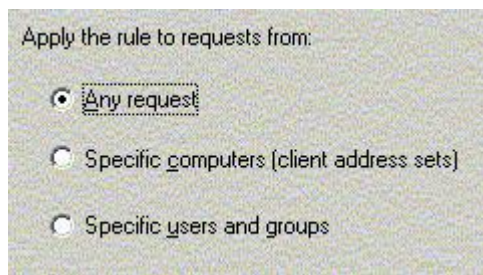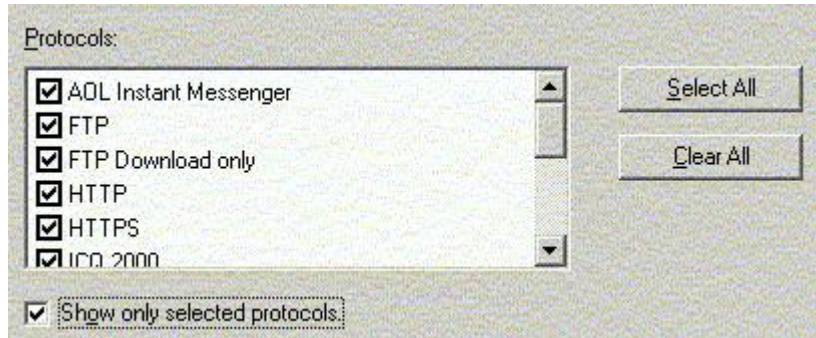
Firewall Configuration Options:

Although ISA_Cache is primarily responsible for processing outbound requests, it still has to defend against outside intrusion. ISA Server relies on packet filtering for its firewall functionalities. On ISA_Cache, packet filtering, intrusion detection and IP routing should be enabled. To be secure, all packet filtering and intrusion detection related options should be enabled as well.

General | Packet Filters | Intrusion Detection | PPTP |

Use this page to control packet routing and packet filtering properties.

☑ Enable packet filtering

  ☑ Enable Intrusion detection
  ☑ Enable IP routing

General | Packet Filters | Intrusion Detection | PPTP |

Use this page to configure packet filter properties.

  ☑ Enable filtering of IP fragments

  ☑ Enable filtering IP options

  ☑ Log packets from 'Allow' filters

For packet filtering, the single most important setting is to deny any requests towards the internal network made by any outside parties. Absolutely no connection initiated from the outside! This can be done by creating "block filter" that stop the external hosts from sending packets to all ports on the ISA Server computer.
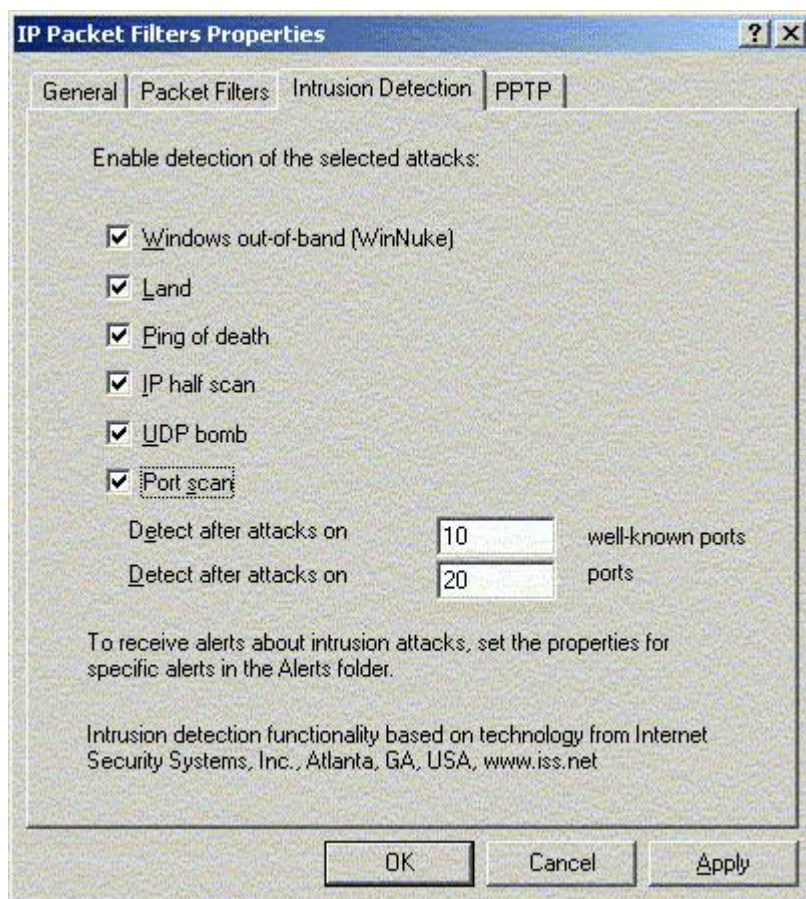
Since the internal clients may be acting as remote VPN clients for accessing the partners' VPN servers, outgoing PPTP traffic should be allowed to pass through the firewall.
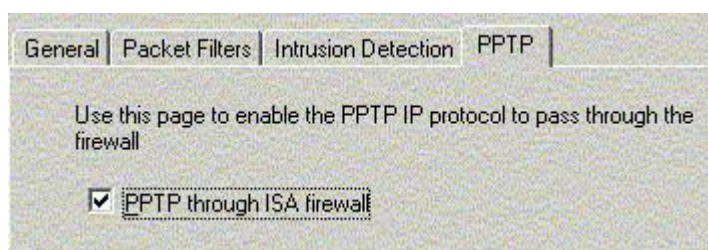
Advanced Caching Options:

To allow room for scalability, multiple ISA servers can be chained to form a larger caching mechanism. Such a mechanism is not needed by GIAC. We do want to ensure that all requests are immediately routed to the destinations rather than to any upstream cache servers. Also, we want to be sure that the HTTP / SSL protocols are not being

transformed into another format when the requests are processed by ISA server. HTTP/SSL should remain as HTTP/SSL even after redirection.
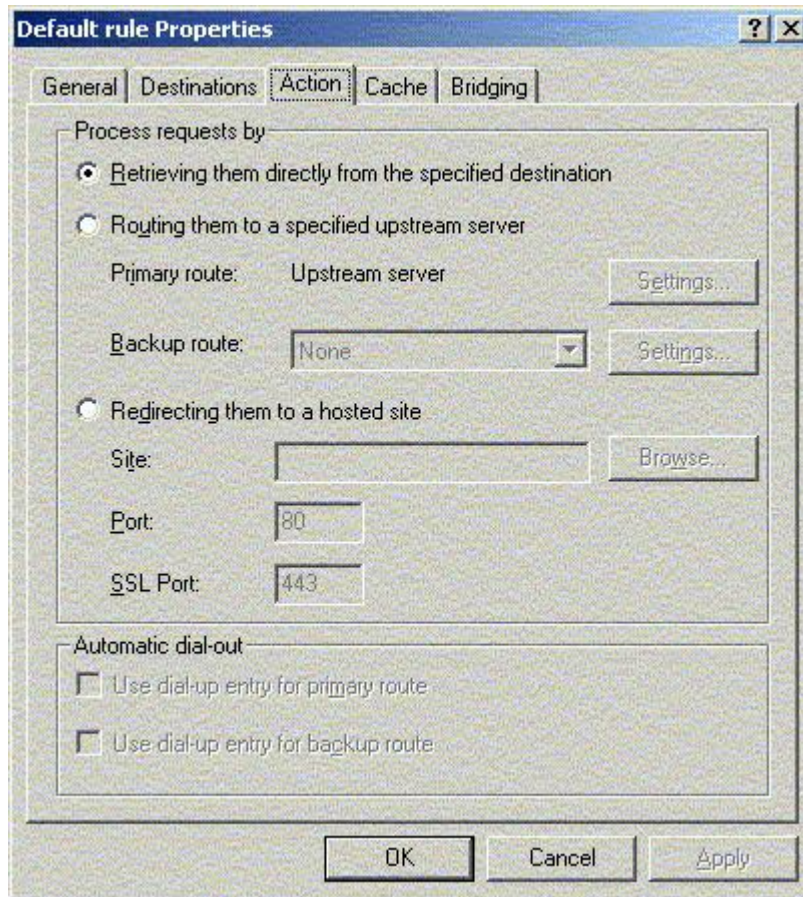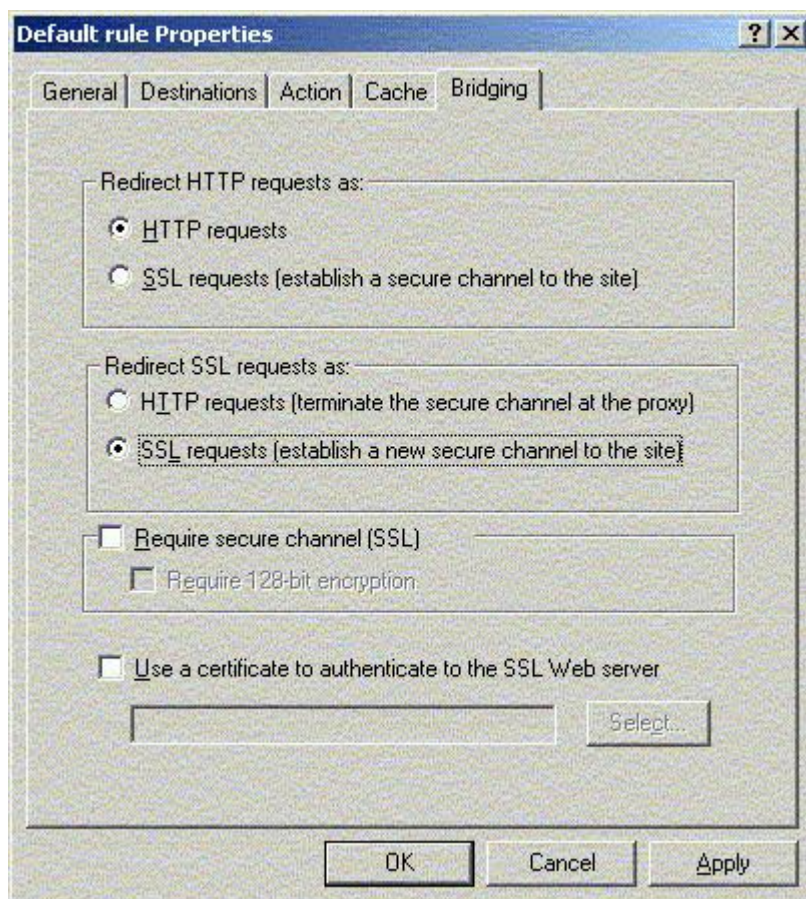
ISA Server supports two major types of caching: HTTP and FTP. There is always a tradeoff between network traffic and content updates. If the cached objects are to be kept in the cache for a longer period of time, performance will increase because less outgoing traffic is required. However, the cached objects may become outdated. The settings can be adjusted in the form of TTL. As described by Webopedia.com,

"Short for Time to Live, (TTL is) a field in the Internet Protocol (IP) that specifies how many more hops a packet can travel before being discarded or returned."[21]

---

[21] http://www.webopedia.com/TERM/T/TTL.html
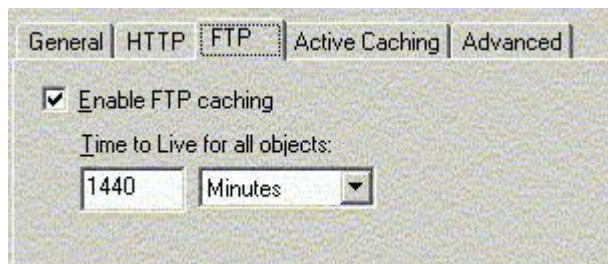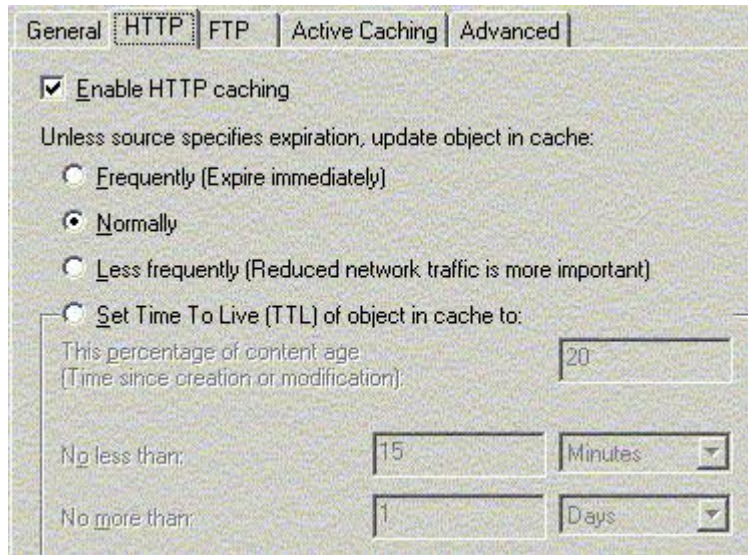
As mentioned before, cached objects may be outdated. For certain objects that involve dynamic contents, caching can be a bad idea. Therefore, do not enable the option "Cache Dynamic Content".
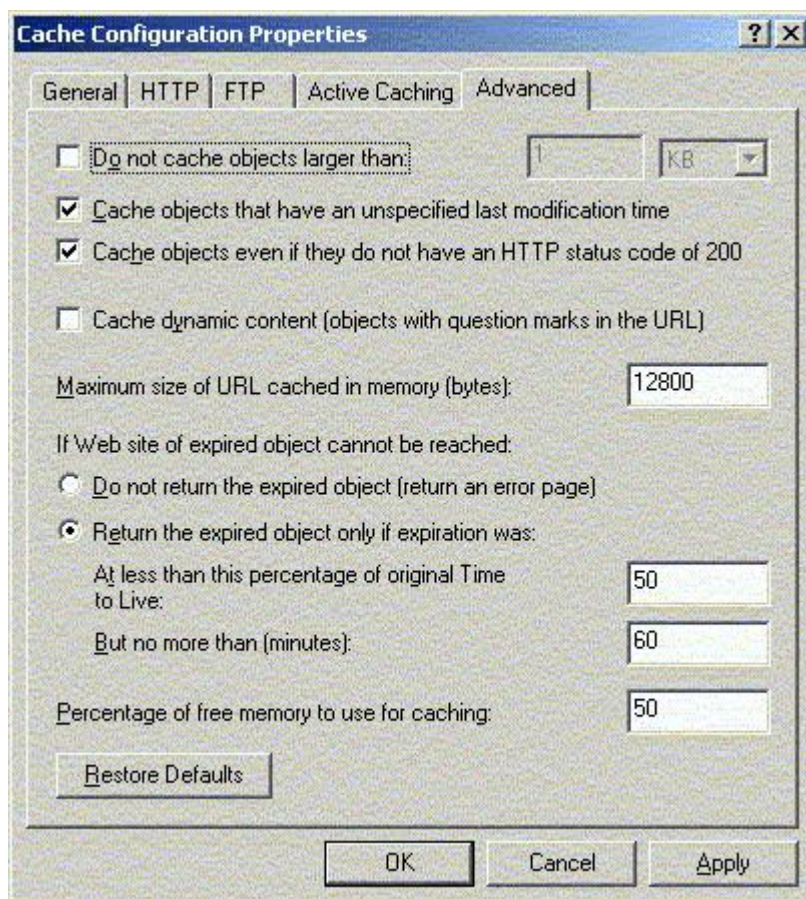
The configured ISA_Cache server will listen on TCP port 8080 as well as SSL port 8443 (SSL port listener must be manually enabled) for outgoing requests. The clients must be configured to forward requests to these ports of the ISA_Cache server's internal interface.

Proxy Filters

To prevent unauthorized users to access these proxy ports, configure input filters to allow connections to be made to TCP 8080 and 8443 only from:

- Internal_Clients
- Internal_Dev
- Internal_Admin
- Internal_Servers

Nothing has to be configured for incoming web requests, as ISA_Cache is not

supposed to handle incoming traffic.
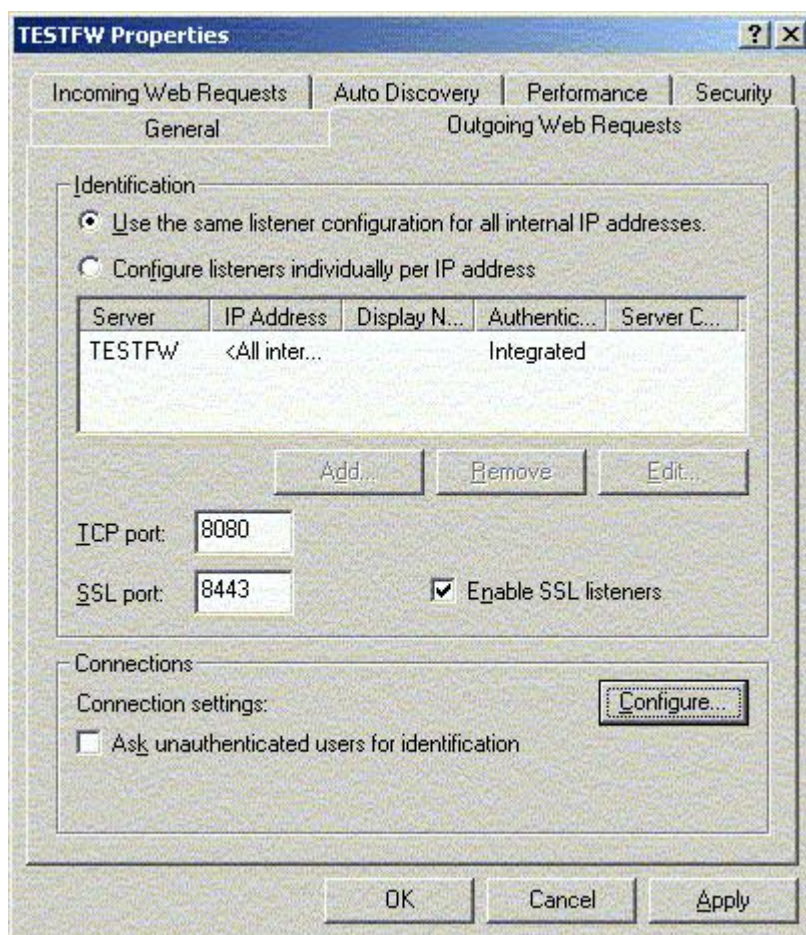
Basic Testing:

■ From Internal_Clients, access an internet web site via ISA_Cache. Such access should succeed.

■ From a non-existing internal subnet, access an internet web site via ISA_Cache. Such access should fail.

■ From the outside world, try to connect to ISA_Cache's proxy port and use it for web access. Such attempt should fail.

■ Inspect the log file.

Further testing should be conducted at the Audit stage.

Configuring the VPN Server

Refer to Assignment1 for information on Windows 2000 hardening.

Short for virtual private network, VPN is a network constructed by using public wires to connect nodes. VPN systems use encryption and other security mechanisms to ensure that only authorized users can access the network and that the data cannot be intercepted[22]. W2K_VPN is a Windows 2000 Server computer running RRAS. It allows a pre-defined number of the remote VPN clients to connect to the Critical_Resources database application server.

Firewall Strategy for the VPN Server:

W2K_VPN sits between Router_Econcard and the core switch / Core_Net. It serves primarily as a VPN Server for accepting remote access requests from the external partners and suppliers. It does not act as a VPN gateway for the internal clients.

There are two approaches to deploying a firewall with a VPN server. We can either place the firewall between the VPN server and the intranet, or place the VPN server between the firewall and the intranet. For GIAC, we go with the first approach: that is, we place the VPN Server in front of the Firewall.

With this strategy, we need to add packet filters to the VPN server's Internet interface to only allow VPN traffic to enter into and going out from the IP address of that interface. For inbound traffic, when the tunneled data is decrypted by the VPN server, it is forwarded to the internal firewall(s) for further filtering and inspection. Since the only traffic crossing the VPN server is generated by authenticated VPN clients, firewall filtering can be used to prevent VPN users from accessing specific intranet resources[23].

---

[22] http://www.webopedia.com/TERM/V/VPN.html

[23] http://www.microsoft.com/windows2000/techinfo/reskit/en-us/default.asp?url=/WINDOWS2000/techinfo/reskit/en-us/intwork/inbe_vpn_HIDV.asp

VPN Model:

A router-to-router VPN model is not deployed primarily because the volume of use between the partnering organizations does not justify a router-router setup. Instead, a Remote Access based VPN solution is deployed to provide maximum flexibility and cost effectiveness.

The paragraph below is extracted from Microsoft's Remote Access VPN Connections document to illustrate this particular type of VPN scenario:

"For dial-up VPN clients who connect to the Internet before creating a VPN connection with a VPN server on the Internet, two IP addresses are allocated:

■ *When creating the PPP connection, IPCP negotiation with the ISP NAS assigns a public IP address.*

■ *When creating the VPN connection, IPCP negotiation with the VPN server assigns an intranet IP address. The IP address allocated by the VPN server can be a public IP address or private IP address, depending on whether your organization is implementing public or private addressing on its intranet.*

In either case, the IP address allocated to the VPN client must be reachable by hosts on the intranet and vice versa. The VPN server must have appropriate entries in its routing table to reach all the hosts on the intranet and the routers of the intranet must have the appropriate entries in their routing tables to reach the VPN clients. The tunneled data sent through the VPN is addressed from the VPN client's VPN server-allocated address to an intranet address. The outer IP header is addressed between the ISP-allocated IP address of the VPN client and the public address of the VPN server. Because the routers on the Internet only process the outer IP header, the Internet routers forward the tunneled data to the VPN server's public IP address."[24]

---

[24]

http://www.microsoft.com/windows2000/techinfo/reskit/en-us/default.asp?url=/WINDOWS2000/techinfo/reskit/en-us/intwork/inbe_vpn_obwd.asp

Security Policy:

The security policies to be enforced here are:

1. Only PPTP connections from the legitimate external partners / suppliers are allowed.
2. No other inbound / outbound traffic types are allowed through this router. That means, drop and log everything else.

Configure W2K_VPN:

Based on the understanding of our VPN model, we can take the necessary steps to configure such a VPN. These steps are:

1. Install hardware in the VPN server
2. Configure TCP/IP on the adapters
3. Install the Routing and Remote Access service
4. Enable any authentication method
5. Configure static routes to reach intranet locations
6. Increase the number of PPTP ports to suit the need of GIAC
7. Configure PPTP packet filters

W2K_VPN has the following interfaces:
■   192.168.6.2 (to Router_Eiconcard)
■   192.168.16.5 (to the core switch / Core_Net)

Before taking the steps to configure this VPN server, it is important for us to harden this system. Information on how to harden Windows 2000 is available in Assignment 1.

Configure RRAS:

To configure VPN on W2K_VPN, we must ensure that it acts as a Remote Access Server. Regarding authentication, we use Windows Authentication as the authentication provider. The corresponding user accounts have to be setup on this

server for the remote users accordingly.
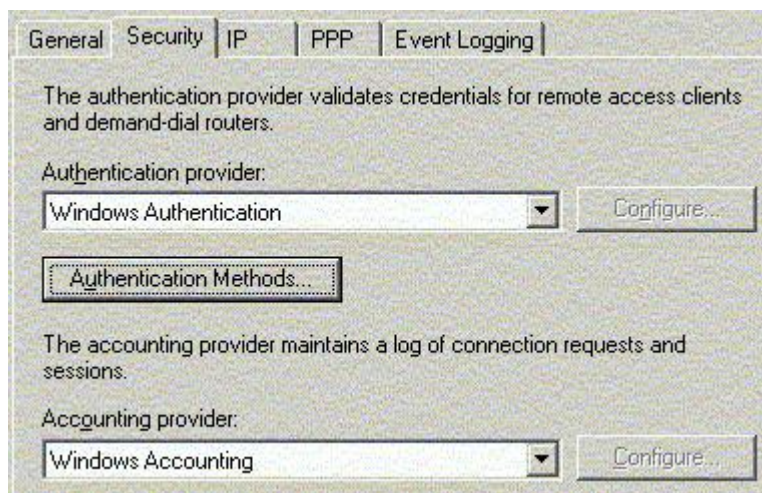
Since the external partners and suppliers are using mostly Windows based clients, MS-CHAP and MS-CHAP V2 are selected as the authentication protocols. According to Chapter 14, Lesson 2 of the Microsoft Press MCSE Training Kit—Microsoft Windows 2000 Network Infrastructure Administration,

"MS-CHAP is a variant of CHAP that does not require a plaintext version of the password on the authenticating server. MS-CHAP passwords are stored more securely at the server but have the same vulnerabilities to dictionary and brute force attacks as CHAP. In MS-CHAP the challenge response is calculated with a Message Digest 4 (MD4)-hashed version of the password and the network access server (NAS) challenge."[25]

---

[25]

http://www.amazon.com/exec/obidos/ASIN/0735613885/qid=1018719524/sr=1-1/ref=sr_1_1/104-955 7570-0347903
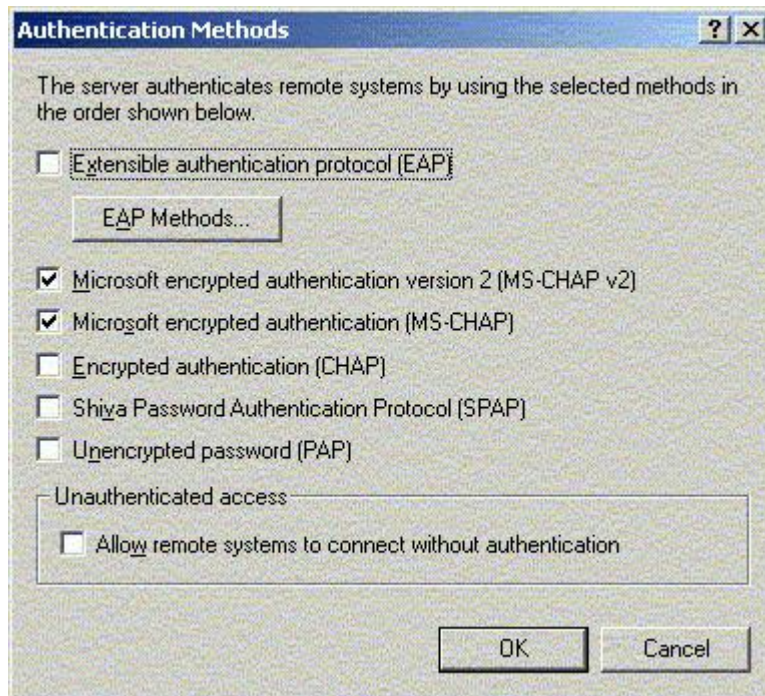
We should then configure W2K_VPN to accept 11 incoming PPTP connections. The number of connections can be increased or decreased on an as needed basis.

External VPN clients are assigned IP addresses from a pool of 11 addresses which belong to the Core_Net subnet. Traffics to the internal network segments are filtered by the other firewalls based on these assigned Core_Net addresses.
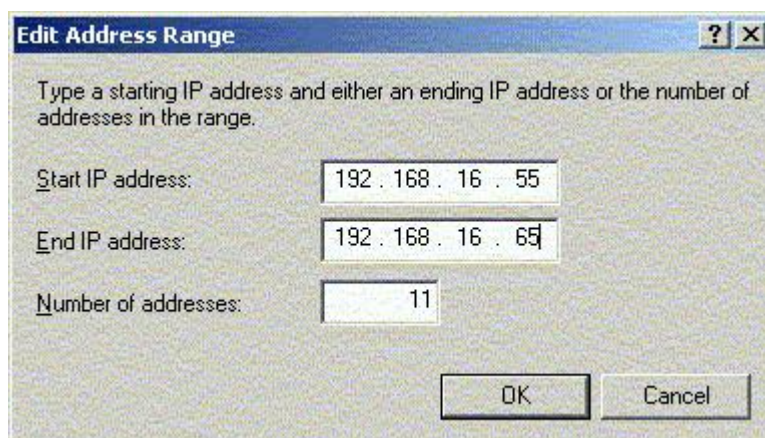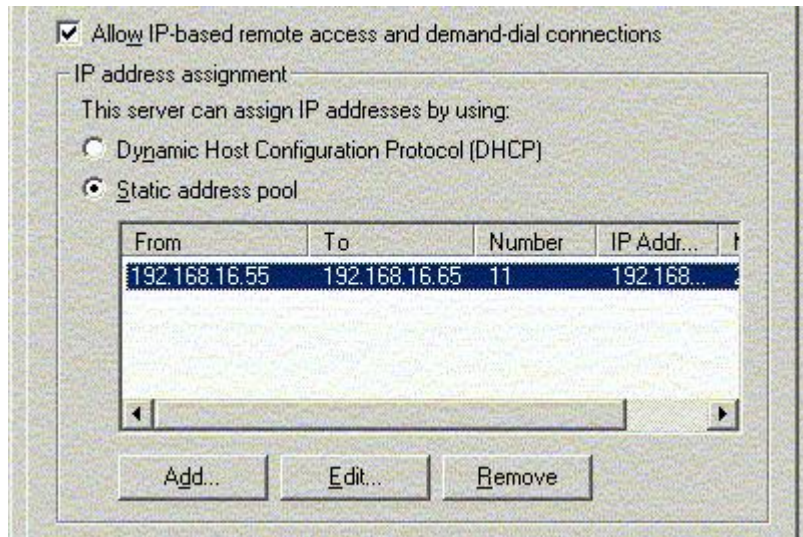
We also want to log as much information about the connections as possible.
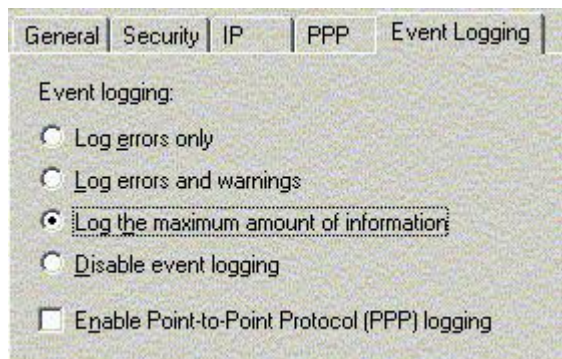
VPN Protocol:

For maximum compatibility, we use PPTP as the choice of tunneling protocol. Known as Point-to-Point Tunneling Protocol, PPTP is developed jointly by Microsoft Corporation, U.S. Robotics, and several remote access vendor companies, and is supported by almost all Windows based clients on earth.

According to Microsoft's PPTP FAQ, the advantages of PPTP are:

"PPTP enables a low-cost, private connection to a corporate network through the public Internet.

PPTP is easy and inexpensive to implement."[26]

PPTP is considered as reasonably secure. According to Chapter 14, Lesson 2 of the Microsoft Press MCSE Training Kit Windows 2000 Network Infrastructure Administration,

"For VPN connections, Windows 2000 uses MPPE with the PPTP, and IPSec encryption with the L2TP. ... MPPE uses the Rivest_Shamir_Adleman (RSA) Rivest's Cipher 4 (RC4) stream cipher and is only used when either the EAP-Transport Layer Security (TLS) or MS-CHAP (version 1 or version 2) authentication methods are used. MPPE can use 40-bit, 56-bit, or 128-bit encryption keys. ...By default, the highest key strength supported by the calling router and answering router is negotiated during the connection establishment process. If the answering router requires a higher key strength than is supported by the calling router, the connection attempt is rejected."[27]

Regarding authentication and encryption under PPTP, refer to the descriptions from Microsoft:

"The user attempting the PPTP connection is authenticated using PPP-based user authentication protocols such as EAP, MS-CHAP, CHAP, SPAP, and PAP. For PPTP connections, EAP-TLS using smart cards or MS-CHAP version 2 is highly recommended as they provide mutual authentication and are the most secure methods of exchanging credentials. ... MPPE can use 40-bit, 56-bit, or 128-bit encryption keys. The 40-bit key provides backward compatibility with non-Windows 2000 clients. By default, the highest key strength supported by the VPN client and VPN server is negotiated during the connection establishment process. If the VPN server requires a higher key strength than is supported by the VPN client, the connection attempt is rejected. ...MPPE for VPN connections changes the encryption key for each packet. The decryption of each packet is independent of the previous packet. MPPE includes a sequence number in the MPPE header. If packets are lost or arrive out of order, the encryption keys are changed relative to the sequence number."[28]

---

[26] http://www.microsoft.com/ntserver/ProductInfo/faqs/PPTPfaq.asp
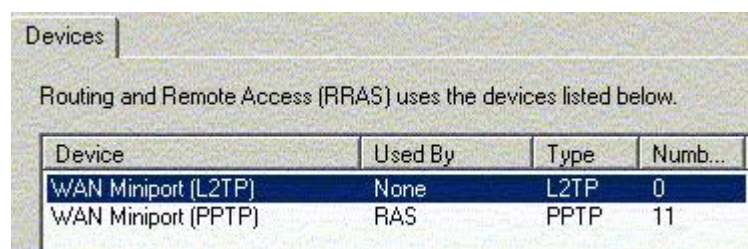
[27] http://www.amazon.com/exec/obidos/ASIN/0735613885/qid=1018719524/sr=1-1/ref=sr_1_1/104-9557570-0347903

[28] http://www.microsoft.com/WINDOWS2000/techinfo/reskit/samplechapters/inbe/inbe_vpn_hueq.asp

Configure the VPN ports and the static route:

By default, RRAS allocates 5 ports for PPTP and 5 ports for L2TP. For GIAC we will use only PPTP, and will configure a total of 11 ports for it. These ports are mapped to the addresses we defined for allocating to the VPN clients.

The final step is to ensure that these external clients can access the Critical_Resources subnet. Microsoft suggests that we use a static route for this purpose. In this case, gateway 192.168.16.6 is used to reach the destination subnet of 192.168.21.0. Since RRAS is running, static route to Critical_Resources should be added via the RRAS MMC console. Using the route add command with the –p switch will not make the entry permanent.

Configure Input Filters:

"A PPTP-based VPN server typically has two physical interfaces: one interface on the shared or public network like the Internet, and another on the private intranet. It also has a virtual interface connecting to all VPN clients. For the VPN server to forward traffic between VPN clients, IP forwarding must be enabled on all interfaces. However, enabling forwarding between the two physical interfaces causes the VPN server to route all IP traffic from the shared or public network to the intranet. To protect the intranet from all traffic not sent by a VPN client, PPTP packet filtering must be configured so that the VPN server only performs routing between VPN clients and the intranet and not between potentially malicious users on the shared or public network and the intranet." (from Microsoft Technet[29])

---

[29] http://www.microsoft.com/WINDOWS2000/techinfo/reskit/samplechapters/inbe/inbe_vpn_hueq.asp

PPTP input packet filters are configured on the adapter that is on the side of the Internet (192.168.6.2).
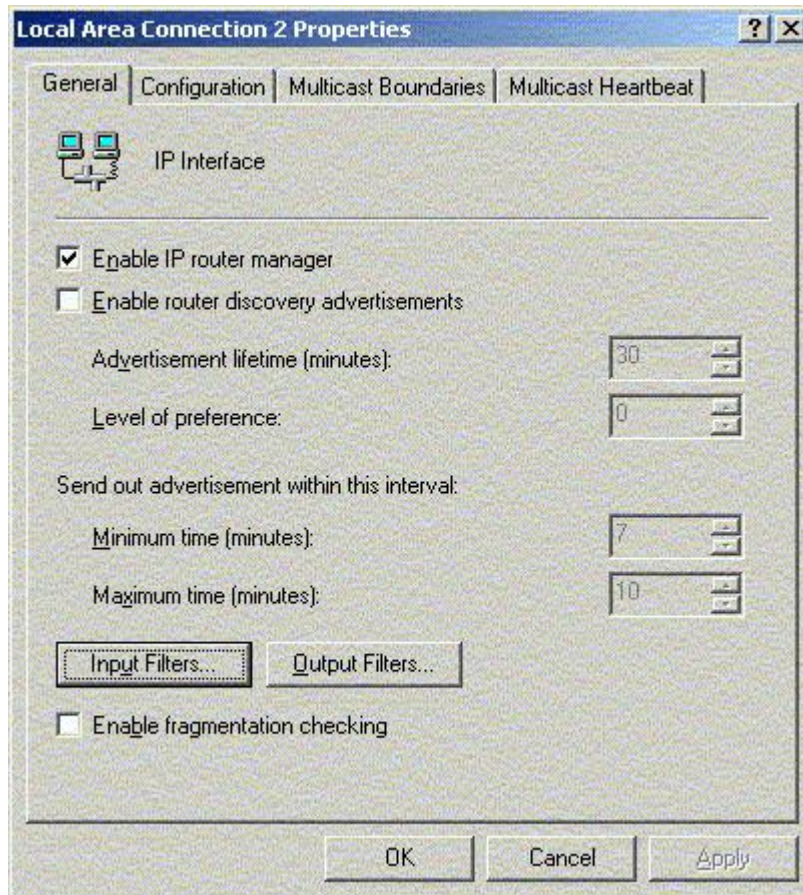
This interface's Input Filters should be configured so that the filter action is set to Drop all packets except those that meet the criteria below:

■ Destination IP address of the VPN server's Internet interface (192.168.6.2), subnet mask of 255.255.255.255, and TCP destination port of 1723. This allows PPTP tunnel maintenance traffic from the PPTP clients to the PPTP server.

■ Destination IP address of the VPN server's Internet interface (192.168.6.2), subnet mask of 255.255.255.255, and IP Protocol ID of 47. This filter allows PPTP tunneled data from the PPTP clients to the PPTP server.

Do not use "TCP [established]" as the port type. This filter is required only if the VPN server is acting as a VPN client (a calling router) in a router-to-router VPN connection in which traffic is accepted only if the VPN server initiated the TCP connection.

For additional protection, we want to set the filters to allow connections only from the external partners / suppliers' IP networks. This requires that the external clients' IP configurations be fully communicated with GIAC.

Configure Output Filters:

PPTP output packet filters are to be configured on the adapter that is on the side of the Internet as well (192.168.6.2).

This interface's Output Filters should be configured so that the filter action is set to Drop all packets except those that meet the criteria below:

- Source IP address of the VPN server's Internet interface (192.168.6.2), subnet mask of 255.255.255.255, and TCP source port of 1723. This allows PPTP tunnel maintenance traffic from the VPN server to the VPN clients.
- Source IP address of the VPN server's Internet interface (192.168.6.2), subnet mask of 255.255.255.255, and IP Protocol ID of 47. This allows PPTP tunneled data from the VPN server to the VPN clients.

Basic Testing:

- Connect from a valid VPN client to Public_Services by going through W2K_VPN. Use L2TP instead of PPTP. The connection attempt should fail.
- Connect from a valid VPN client to Public_Services by going through W2K_VPN. Use PPTP. Access the database application using HTTP. The connection attempt should succeed.
- Connect from a non-valid VPN client to Public_Services by going through W2K_VPN. Use PPTP. Access the database application using HTTP. The connection attempt should fail.
- Inspect the RAS log file.

Further testing should be conducted at the Audit stage.

Configuring Basic Filters on Router_Eiconcard:

Router_Eiconcard is the router for internet connectivity. It is equipped with Eiconcard model S92, which supports 2 high speed WAN ports, each at T1 speed. The software that comes with it is Eiconcard Connections for Windows 2000. By closely integrating with Windows 2000 RRAS, routing and basic filtering can be configured to support the GIAC network.
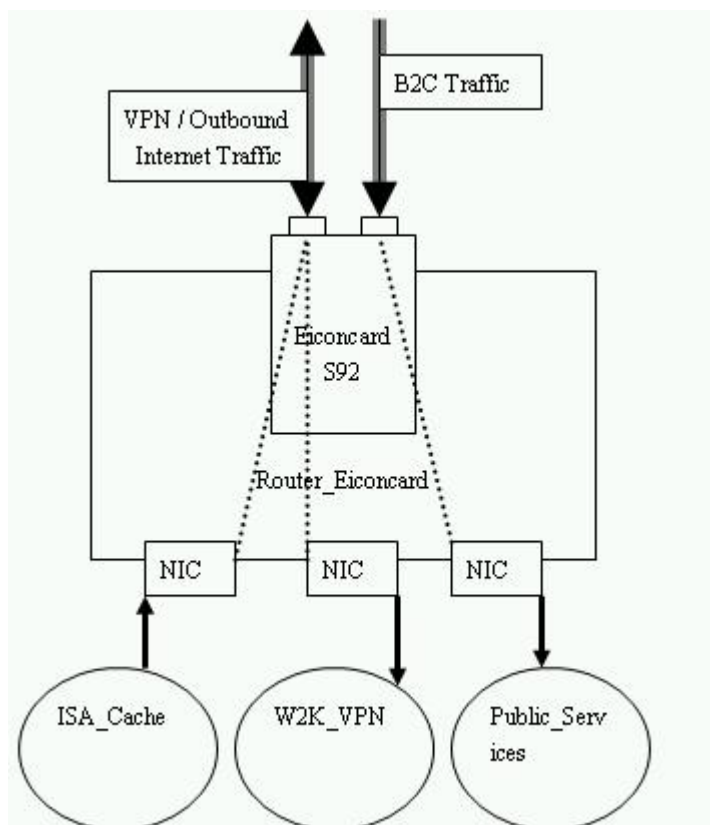
Security Policy:

The basic security function at Router_Eiconcard is anti-spoofing. Packets coming in from the internet are inspected against spoofing.

Filtering at Router_Eiconcard:

Refer to the "Products Preparation" section for information on Eiconcard S92.
Refer to the "Products Preparation" section for information on Windows 2000 hardening.

With Eiconcard Connections for Windows 2000, all packets are forwarded for a connection for which no IP packet filters is created. However, building too many filters can be costly as more processing has to be done for every packet handled. We definitely do not want Router_Eiconcard to become the network bottleneck.
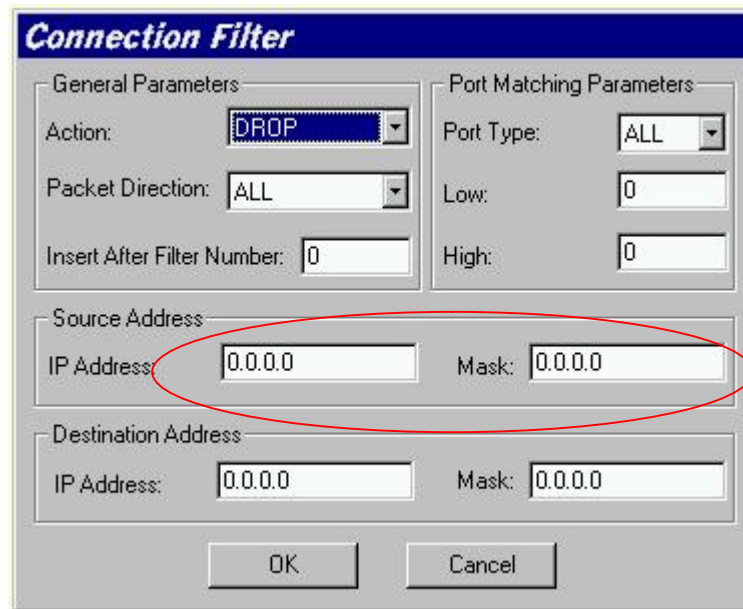
Rules and Orders

Since all internal segments are protected by multiple layers of firewall, screening activities at Router_Eiconcard should be restricted to only dropping incoming internet traffic that has source addresses belonging to GIAC's internal IP subnets (we do this to protect the network against spoofing attack). **This way delay can be minimized at this choking point of the network.**

According to webopedia.com, spoofing is:

"a technique used to gain unauthorized access to computers, whereby the intruder sends messages to a computer with an IP address indicating that the message is coming from a trusted host. To engage in IP spoofing, a hacker must first use a variety of techniques to find an IP address of a trusted host and then modify the packet

headers so that it appears that the packets are coming from that host."[30]

Detailed information on IP Spoofing is available at:

IP-spoofing Demystified: http://www.fc.net/phrack/files/p48/p48-14.html

To prevent incoming IP packets labeled with "internal" IP addresses from entering the network via the WAN adaptor, configure filters on the WAN adaptor S92 with each Direction set to IN, Action to Drop, Source IP Address to the internal addresses, and Source Mask to 255.255.255.255:

IN, DROP, Source: Core_Net (192.168.16.0), Mask: 255.255.255.255

IN, DROP, Source: Public_Services (192.168.8.0), Mask: 255.255.255.255

IN, DROP, Source: Internal_Clients (192.168.17.0), Mask: 255.255.255.255

IN, DROP, Source: Internal_Servers (192.168.18.0), Mask: 255.255.255.255

IN, DROP, Source: Internal_Admin (192.168.19.0), Mask: 255.255.255.255

IN, DROP, Source: Internal_Dev (192.168.20.0), Mask: 255.255.255.255

IN, DROP, Source: Critical_Resources (192.168.21.0), Mask: 255.255.255.255

IN, DROP, Source: RAS_Net (192.168.22.0), Mask: 255.255.255.255

The filters are processed sequentially. For our rules, since the addresses do not overlap, there are no conflicts between them, and the order would therefore be irrelevant.

Basic Testing

■ Configure a client with an address from Internal_Clients. Connect from the outside to the WWW server in Public_Services via HTTP. The packet should be dropped right at Router_Eiconcard.

■ Configure a client with an address from Internal_Dev. Connect from the outside to the DNS server in Public_Services via NSLOOKUP. The packet should be dropped right at Router_Eiconcard.

■ Configure a client with an address from the outside world. Connect from the outside to the WWW server in Public_Services via HTTP. The packet should be allowed to pass through at Router_Eiconcard.

■ From a valid client in Internal_Admin, connect to the outside world. The request

---

[30] http://www.webopedia.com/TERM/s/spoof.html

should be allowed to pass through at Router_Eiconcard.

■   Inspect the log file.

In-depth testing should be performed at the Audit stage.

Configuring the RAS Server

The RAS_Net RAS server is a "backdoor" to the network. It allows the company staffs to remote accessing the server resources in Internal_Servers as well as to access the company's Public_Services servers. Users without formal accounts in the domain controller are not allowed to log in via RAS.

Security Policy:

1. Only legitimate users with the valid credentials and from the valid dialing locations are allowed to login.
2. Disallow everything else.

RAS Configuration:

This RAS server will be configured with a pool of 5 modems and 5 client IP addresses (that belongs to the RAS_Net subnet) for allocation to the dial-in clients. These clients are forced to take and use these addresses. The corresponding firewall filters at VisNetic_1 are configured based to make filtering decisions based on these addresses.

To make sure that this RAS server does not constitute a security hole, we must:

■ Take steps to harden this Windows 2000 system. Refer to the "Products Preparation" section for information on how to proceed.
■ Configure the corresponding Remote Access Policies and requires strong encryption as well as strong authentication.
■ Configure account lockout policy to restrict the number of login attempts allowed.
■ Configure the system to accept incoming calls only from pre-defined numbers, and use call-back security to ensure that only the "true employees" and no one else can dial in.

With remote access policies, a connection is authorized only if the settings of the connection attempt to match at least one of the remote access policies. According to

the Online Documentation provided by Microsoft,

"In Windows 2000, authorization is granted based on the dial-up properties of a user account and remote access policies. Remote access policies are a set of conditions and connection settings that give network administrators more flexibility when authorizing connection attempts... With remote access policies, you can grant or deny authorization by time of day or day of the week, by the Windows 2000 group to which the remote access user belongs, by the type of connection being requested (dial-up networking or VPN connection), and so on. You can configure settings that limit the maximum session time, specify the authentication and encryption strengths, set Bandwidth Allocation Protocol (BAP) policies, and so on."[31]

For client-end authentication, smart card should be mandatory. This is possible, according to Microsoft, when EAP is deployed:

"The Extensible Authentication Protocol (EAP) is an extension to the Point-to-Point Protocol (PPP) that allows arbitrary authentication methods using credential and information exchanges of arbitrary lengths... By using EAP, support for a number of specific authentication schemes known as EAP types may be added, including token cards, one-time passwords, public key authentication using smart cards, certificates, and others."[32]

Basic Testing:

- Dial in from a valid phone number with a valid user account. Wait for the call back and try to log on. The attempt should succeed.
- Dial in from a non-valid phone number with a valid user account. Wait for the call back and try to log on. The attempt should fail.
- Dial in from a valid phone number with a non-valid user account. Wait for the call back and try to log on. The attempt should fail.
- Inspect the RAS log file.

---

[31]

http://www.microsoft.com/windows2000/techinfo/reskit/en-us/default.asp?url=/WINDOWS2000/techinfo/reskit/en-us/deploy/dgcf_inc_bhah.asp

[32]

http://www.microsoft.com/windowsxp/home/using/productdoc/en/default.asp?url=/WINDOWSXP/home/using/productdoc/en/auth_eap.asp

More in-depth testing should be performed at the audit stage.

Special Consideration - the Email Server

Email security is a major issue in nowadays security context. Even with the help of firewalls, email threats are not easy to be avoided. These threats include malicious contents, spam and viruses. To be able to truly secure the email service, it is important to deploy an email server solution which by itself is strong and secure. One such recommended solution is MDaemon. As described by Deerfield:

"MDaemon is a scalable mail server with built-in content filtering, spam blocking and support for AntiVirus Plug-in. This standards-based SMTP, POP and IMAP server meets the email needs of any group, regardless of size and features a powerful set of integrated tools for managing mail accounts and message formats… At the enterprise level, MDaemon allows administrators to manage and secure email internally."[33]

The Antivirus plug-in of MDaemon
(http://www.deerfield.com/products/mdaemon/antivirus/) can detect all known viruses including plain text attachments and HTML messages, as well as to control the content entering the network by scanning the subject and body of an email.

---

[33] http://www.deerfield.com/products/mdaemon/

Assignment 3

The Security Audit

Overview

"Firewalls are great for restricting access to your network, but firewalls cannot prevent all problems."(from Securityspace.com[34])

According to Securityspace.com, the most common problems with firewalls are:

- firewall misconfiguration
- vulnerable network services

The goal of our security architecture audit is to verify that the defense mechanism we design for GIAC is functioning properly. Such a comprehensive audit shall include the following elements as described by wemanageservers.com:

"Footprint Analysis - what operating system and what services and applications are running on it.
Port Scanning - what ports are open that can allow potential connection to the system?
Vulnerability Analysis - what areas of the system can be exploited by hackers?
Penetration Testing - Attempt to exploit vulnerabilities found in the vulnerability analysis phase."[35]

In a full scale audit, even the hosts behind the firewalls are to be tested. For the scope of this project, however, our effort will be limited to the routers and the firewalls.

Depth of the Audit

To isolate and clearly identify the weaknesses or flaws of every security device in the network, each device is tested independently against what are to be expected out of each of them. To be precise, we want to find out:

---

[34] http://www.securityspace.com/smysecure/daudit_faq.html
[35] http://www.wemanageservers.com/managed_security/security_audit/security_audit.html

- any vulnerability exist in the security devices
- whether the security policies are properly implemented and enforced by the security devices

Network scanning is the primary method to use, in addition to manual connection attempts and procedure review for verifying the security rules and operations. This audit, however, is not budgeted to perform in-depth penetration.

In fact, hiring the expertise of a professional penetration team to perform penetration testing against the high risk area (such as the B2C stream) is an option that deserves further consideration[36].

Phrases

The phrases involved in our security audit include:

Phrase 0 – Planning and Preparation
At this phrase we need to get ourselves familiar with the organization and the network, prepare the necessary paperwork and tools and devise an audit plan for approval.

Phrase 1 - Organization Review
In this phrase we review the existing security policies and procedures in place, and determine if they are being followed in the day-to-day operation. Relevant information can be collected through interviews (with the employees), observations and documentation reviews. The focus is more on the "human" side.

IN CERTAIN CIRCUMSTANCES, A REVIEW OF THE EXISTING SECURITY POLICIES IS NEEDED. WE WANT TO ENSURE THAT THESE SECURITY POLICIES PROPERLY SATISFY THE NEEDS OF THE ENTERPRISE IN AN UP-TO-DATE MANNER.

Phrase 2 – Technical Assessment from an "Insider" perspective
In this phrase we mainly concern with the defense mechanism at the departmental level.

---

[36] "Hiring a Penetration Testing Team", Hack Proofing Your E-commerce Site, ISBN: 1-928994-27-X, http://www.syngress.com/catalog/sg_main.cfm?pid=1216

Each network should be tested from the internal user networks to ensure that safety exists internally, that malicious attempts from the internal users are being restricted. Each installed security configuration that is to be tested must first be reviewed to determine the service packs / patches status. The settings must be compared with the latest list of vulnerabilities to see if further action is necessary.

Phrase 3 – Technical Assessment from an "Outsider" perspective

In this phrase we will act like the outside hackers who try to find ways into our private network. Again, each installed security configuration that is to be tested must first be reviewed to determine the service packs / patches status. The settings must be compared with the latest list of vulnerabilities to see if further action is necessary.

Phrase 4 – Administrative Assessment and Fault Tolerance Assessment

In this phrase we focus on auditing the "admin" aspect of the security solutions in place, as well as to review the current level of fault tolerance.

Phrase 5 – Report Preparation

In this phrase we prepare a report on the findings and recommendations. This report will be submitted to the management.

Phrase 6 – Follow up
In this phrase we follow up to ensure that any identified shortcoming is to be taken care of.

As auditors, we do NOT fix the problems ourselves. Instead, we identify the problems and give recommendations to the auditee.

Coordination, Staffing and Schedule

We need to complete the audit effectively without introducing significant disruption to the daily operations. At the same time, we do not want to incur an extraordinary large expense for this purpose. The ideal arrangement in this case is:

Number of Staff:

- 3

Time budget:

- 1 day for Phrase 0
- 1 day for Phrase 1
- 1 day for Phrase 2
- 1.5 days for Phrase 3. The reason why more time is allocated to Phrase 3 is because this assessment involves area with the highest risks (the public service area).
- 0.5 day for Phrase 4
- 0.5 day for Phrase 5
- After completion, time will be separately allocated to the Phrase-6 follow-up activities.

Schedule:

- Phrase 0 – Thursday.
- Phrase 1 – Friday – this is usually the less busy day.
- Phrase 2 – Saturday – such a test is better to be performed in non-office hours.
- Phrase 3 – Saturday nite and Sunday – such a test is better to be performed in non-office hours.
- Phrase 4 & 5 – Monday.
- Phrase 6 – to be arranged after audit completion.

Cost:

- "One man day" cost of USD$800 (taken into account weekend work extra pay and other allowances) x 3 staffs x 5.5 days = USD$13200

Before anything is started, it is important that the following be achieved:

1. Obtain top management approval
2. Coordinate with departmental heads in terms of schedules and resources
3. Notify the staffs in advance about the audit. Have them backup their important files just in case something goes wrong during the audit.

Tools of the Trade

To perform an audit against the firewall systems, we need the help of some software tools. These tools can be classified into two categories: Scanning tools and Stress Test tools. To ensure accurate results, for each type of test we use products of identical nature from at least two different vendors. Different result sets can then be consolidated for further analysis.

This is especially true for scanning. Different scanners use different technologies and target port lists, which for sure will deliver different results. One might argue that such disagreement in results can be minimized by instructing the scanner to scan through every single port. Such strategy is technically possible, but is extremely time consuming and is not practical in our situation.

Scanners:

- for the discovery of network and system vulnerabilities
- suitable for broad scanning at the network level against the frontline routers and firewalls

Retina (based on NMAP technology)

Retina is a commercial audit tool based on the NMAP technology.

"Acknowledged as the fastest vulnerability assessment scanner on the market today, Retina is designed scan any machine on an internet, intranet, or extranet network in order to identify existing vulnerabilities and check adherence of established security policies. Retina provides help on fixing identified vulnerabilities, and produces a

comprehensive report of each scan."(from www.eEye.com[37])

Retina is used in our project as the primary scanning tool. The reasons are:

1, Retina supports an extensive set of audits, including:
- Accounts
- CGI Scripts
- CHAM
- Commerce
- Dns Services
- DoS
- FTP Servers
- IP Services
- Mail Servers
- Miscellaneous
- NetBIOS
- Registry
- Remote Access
- Rpc Services
- Service Control
- SNMP Servers
- SSH Servers
- Web Servers

(http://www.eeye.com/html/Support/Retina/RTHs/index.html)

2, Retina supports the use of Artificial Intelligence technology for simulating real world hacking processes:

"CHAM (Common Hacking Attack Methods):
This groundbreaking feature is the first of its kind. CHAM employs AI technology in order to simulate the thought process of a hacker or security analyst in finding holes in networks and software packages. CHAM enables Retina to go beyond looking for known vulnerabilities. By simulating the approach and thought process of a hacker, CHAM is able to identify unknown vulnerabilities in networks. Set it loose on your web server, or on custom application being developed by your engineers. eEye uses

---

[37] http://www.eeye.com/html/Products/Retina/index.html

CHAM in its own vulnerability research efforts and has been invaluable in enhancing its capabilities in releasing many such advisories."(from www.eEye.com[38])

3, Retina supports OS detection that can accurately determine the OS platform of the target system.

We especially want retina to try to detect the firewall / router type when performing the port scan. When a firewall / router's identity is revealed to Retina, that means additional security measure is necessary … if the hacker knows what firewall/router we are using, it will be much easier for him/her to focus the attack effort.

To take full advantages of Retina's capabilities, some options must be configured for the most extensive scanning. These include:

Complete Scan – Enable Force Scan. Enable all 4 options of CHAM, including FTP, POP3, SMTP and HTTP.
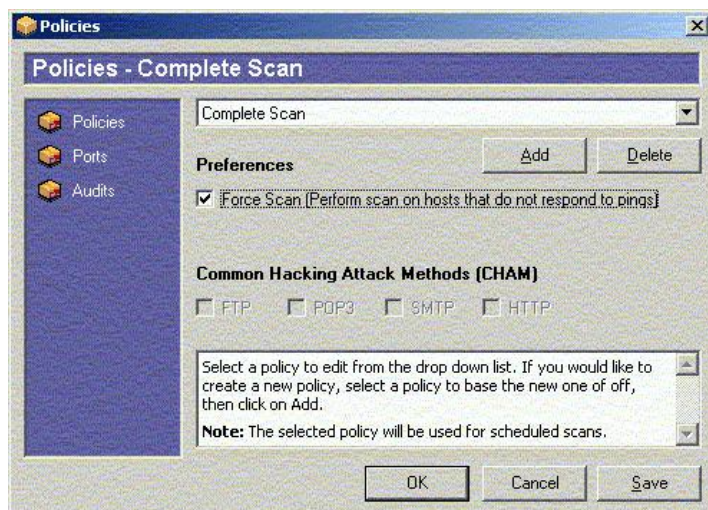
Check all – scan all the ports in the list.
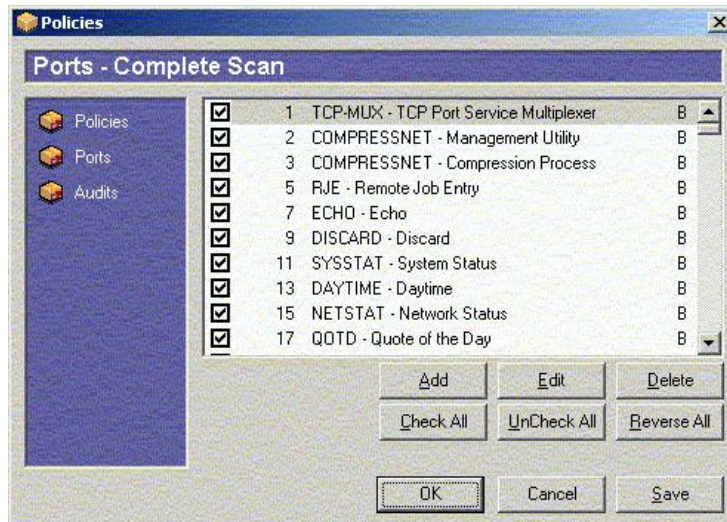
Select all the audit options.
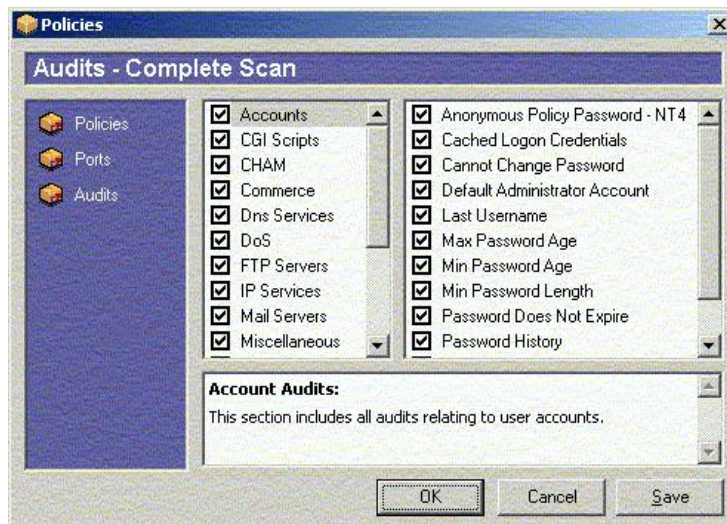
SuperScan

"A powerful connect-based TCP port scanner, pinger and hostname resolver. Multithreaded and asynchronous techniques make this program extremely fast and versatile." (from www.foundstone.com[39])

---

[39] http://www.foundstone.com/knowledge/proddesc/superscan.html

NetBrute

"NetBrute allows you to scan a single computer or multiple IP addresses for available Windows File & Print Sharing resources. This is probably one of the most dangerous and easily exploitable security holes. It is common for your novice users to have their printers or their entire hard drive shared without being aware of it. This utility will help you to find these resources, so you can secure them with a firewall or by informing your users how to properly configure their shares with tighter security." (from www.rawlogic.com[40])

"Exposed shares" are problems most likely found "internally" (as resource sharing is exercised on a daily basis by the LAN clients and servers). Although the public service servers do not need to provide any resource sharing facility, careless configuration on these servers can make exposed shares possible.

Share Scanner

"Share Scanner is a graphical utility that will allow you to view shares on a remote machine. Share Scanner uses windows networking to view these shares (which is unfortunately extremely slow), so it is best to set your timeout to 0 so that it takes as long as it must to find out this information." (from www.mikersoft.com[41])

Same as NetBrute, Share Scanner is used for detecting Microsoft networking shares.

Sub-Net 2.0

"Sub-Net 2.0 is a trojan horse port scanner. A good program to analyze your internet connection or any other machines on your network for over 150 backdoor attacks. At a fast scanning speed of less than 20 seconds you will be able to scan yourself before an attacker gets a chance to connect to your computer." (from www.sub-seven.com[42])

---

[40] http://www.rawlogic.com/products.html
[41] http://www.mikersoft.com/ant/ant_help_shares.html
[42] http://www.sub-seven.com/freeware.shtml

A Trojan is a destructive program that masquerades as a benign application. According to webopedia.com:

"Trojan horses do not replicate themselves but they can be just as destructive. One of the most insidious types of Trojan horse is a program that claims to rid your computer of viruses but instead introduces viruses onto your computer.[43] "

As Trojan attack becomes increasing common, we need to pay special attention to such threat. After any potential Trojan port is detected by Sub-Net, double confirm the result using the list made available by DOShelp[44].
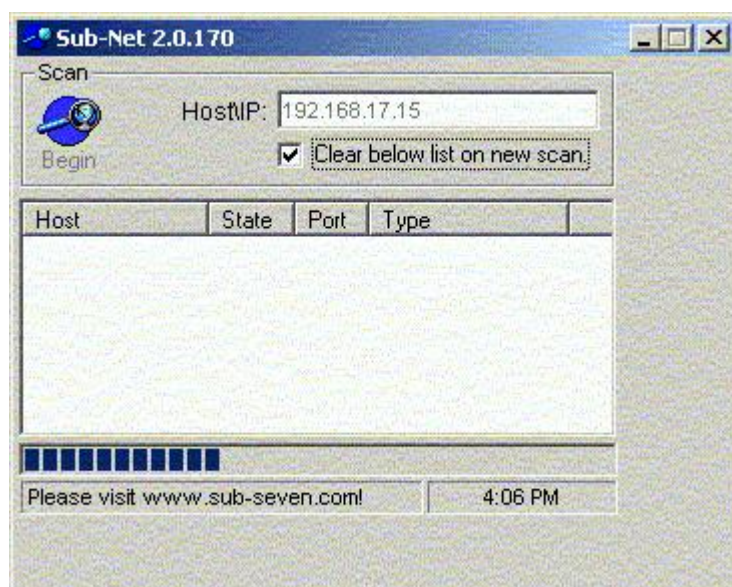
Stress test tools

Every firewall solution includes a combination of hardware and software. As every combination is unique, there is no guarantee that every one of them can stand against the tough real world challenge. Therefore, we use the Stress test tools:

- for producing the effect of DoS attack
- to find out if the heavy traffic can break the firewall

---

[43] http://www.webopedia.com/TERM/T/Trojan_horse.html
[44] http://www.doshelp.com/trojanports.htm

UDPFlood

"A UDP packet sender. It sends out UDP packets to the specified IP and port at a controllable rate. Packets can be made from a typed text string, a given number of random bytes or data from a file." (from www.foundstone.com[45])
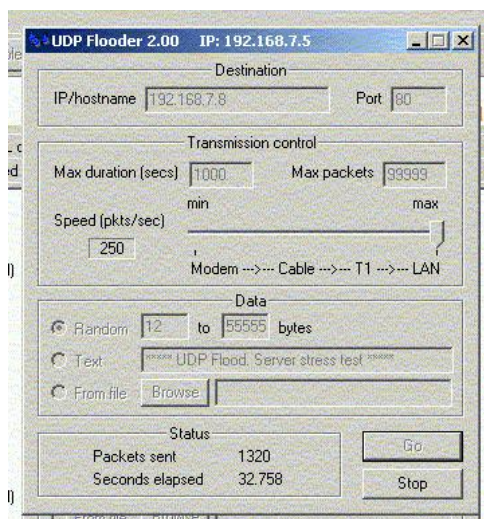
Web Server Stress Tools

"Most web applications run smoothly and correctly as long as only one user (often the original developer) is using it. But what happens when thousands of users access the web site simultaneously?! Webserver Stress Test Tool simulates simultaneous users accessing a web server and helps to streamline your web application." (from web-server-tools.com[46])

---

[45] http://www.foundstone.com/knowledge/proddesc/udpflood.html
[46] http://web-server-tools.com/WebStress/webstress.htm
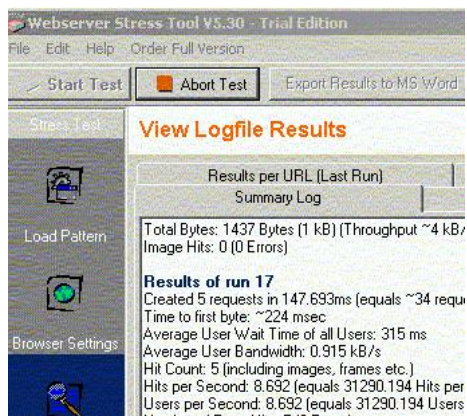
Assessment – from an "Insider" perspective

Since there are time and resource constraints, we cannot test everything for every single possibility. Instead, we need to define a series of tests which are "right to the point".

The attack routes:

First of all, we identify the possible attack routes and build the following test scenarios. Since it is not likely for DoS attack to happen from the inside (it is too easy to be detected and eliminated via Network Monitor), stress tests are not conducted for the scenarios below.

Test scenarios:

Scenario One: Attacker trying to access the various GIAC's internal server resources.
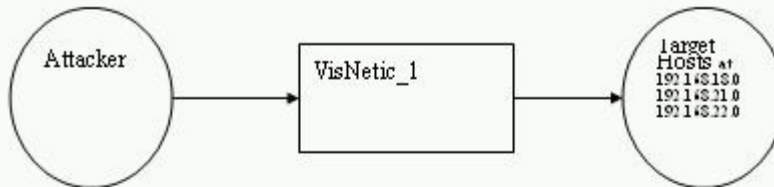
Attacker → VisNetic_1 → Target Hosts at 192.168.18.0 192.168.21.0 192.168.22.0

Scenario Two: Attacker trying to access the staffs' desktops.

Attacker → Norton1/2/3_IDS → Target Hosts at 192.168.17.0 192.168.19.0 192.168.20.0

Scenario Three: Attacker trying to tamper with the public service servers.

Attacker → FW2_B2C → Target Hosts at 192.168.8.0

Scenario Four: Attacker trying to login via RAS.

Attacker → RAS Server

Scenario One:

```
Scenario One: Attacker trying to access the various GIAC's internal
server resources.
```

Attacker → VisNetic_1 → Target Hosts at
192.168.18.0
192.168.21.0
192.168.22.0
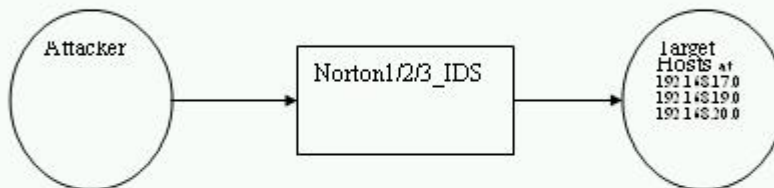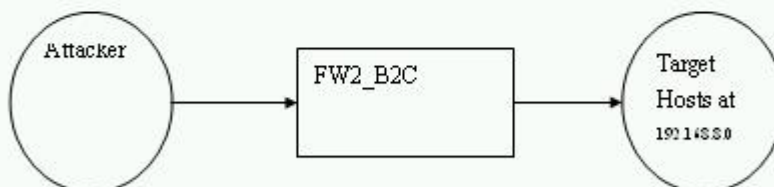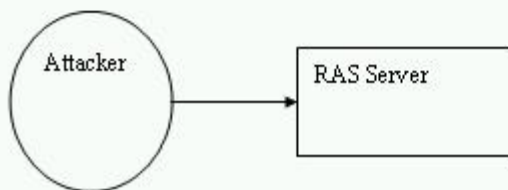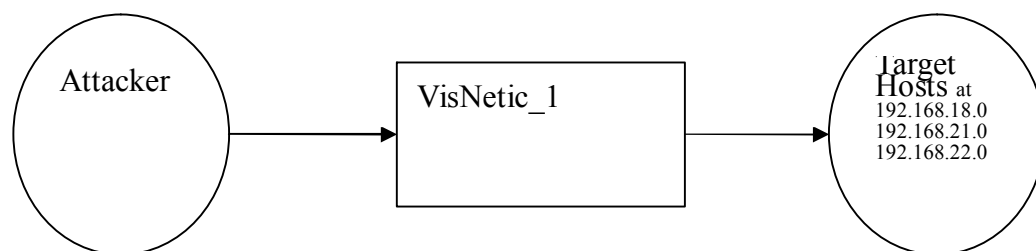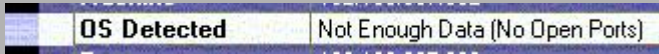
Segments involved: Core_Net (192.168.16.0), Internal_Servers (192.168.18.0), Critical_Resources (192.168.21.0), RAS_Net (192.168.22.0)

Remarks:

- Scanning will be targeted directly towards the firewall itself and the hosts behind it.
- The target hosts include all servers in Internal_Servers, the RAS server and the critical database application server.
- Share scanning is not to be performed against the servers in Internal_Servers, as the subnet is designed to house all the shares, that shares are expected.

Scan from	Target(s)	Tool	Ports/Shares discovered	Intrusion logged	Comments / Recommended actions
192.168.16.99	VisNetic_1	SuperScan	Nil	Yes	
192.168.16.99	192.168.18.0	SuperScan	Nil	Yes	
192.168.16.99	192.168.21.0	SuperScan	Nil	Yes	
192.168.16.99	192.168.22.0	SuperScan	Nil	Yes	
192.168.16.99	VisNetic_1	Retina	All the allowed service ports plus port 81, 82, 83, 1025 and 1031. * OS cannot be detected.	Yes	The details of these detected ports are: hosts2-ns 81/tcp HOSTS2 Name Server hosts2-ns 81/udp HOSTS2 Name Server xfer 82/tcp XFER Utility xfer 82/udp XFER Utility mit-ml-dev 83/tcp MIT ML Device mit-ml-dev 83/udp MIT ML Device 1025/tcp network blackjack 1025/udp network blackjack 1031/tcp BBN IAD 1031/udp BBN IAD A research on VisNetic shows that there is no vulnerability (related to these ports) reported. However, it is recommended that these ports be

blocked via the interface's port filter, since we never know when a new vulnerability will come true.

The fact that the OS type of the firewall is successfully hidden deserves a highly positive comment.

| OS Detected | Not Enough Data (No Open Ports) |

192.168.16.99	192.168.18.0	Retina	Nil	Yes
192.168.16.99	192.168.21.0	Retina	Nil	Yes
192.168.16.99	192.168.22.0	Retina	Nil	Yes
192.168.16.99	VisNetic_1	NetBrute	Nil	Yes
192.168.16.99	192.168.21.0	NetBrute	Nil	Yes
192.168.16.99	192.168.22.0	NetBrute	Nil	Yes
192.168.16.99	VisNetic_1	Share Scanner	Nil	Yes
192.168.16.99	192.168.21.0	Share Scanner	Nil	Yes
192.168.16.99	192.168.22.0	Share Scanner	Nil	Yes
192.168.16.99	VisNetic_1	Sub_Net	Nil	Yes
192.168.16.99	192.168.21.0	Sub_Net	Nil	Yes
192.168.16.99	192.168.22.0	Sub_Net	Nil	Yes

Rulebase assessment

As an external partner, connect as a valid VPN client and access all the segments OTHER THAN the Critical_Resources segment.	**Connections failed. This is the desirable result.**
As an external partner, connect as a valid VPN client and access the Critical_Resources segment via any protocol OTHER THAN HTTP/HTTPS.	**Connections failed. This is the desirable result.**
From Internal_Dev, access Critical_Resources via any protocol OTHER THAN HTTP/HTTPS.	**Connections failed. This is the desirable result.**
From Internal_Clients, access Critical_Resources via any protocol OTHER THAN HTTP/HTTPS.	**Connections failed. This is the desirable result.**
As a RAS user, login via RAS, then connect from RAS_Net to Critical_Resources via HTTP/HTTPS.	**Connections failed. This is the desirable result.**

Scenario Two:

Scenario Two: Attacker trying to access the staffs' desktops.

Attacker → Norton1/2/3_IDS → Target Hosts at 192.168.17.0 192.168.19.0 192.168.20.0
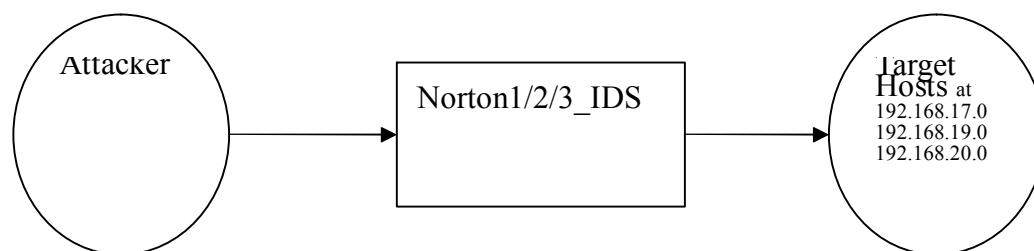
Involved segments: Core_Net (192.168.16.0), Internal_Clients (192.168.17.0), Internal_Admin (192.168.19.0), Internal_Dev (192.168.20.0)

Remarks:

■ Scanning will be targeted directly towards the firewalls themselves as well as the hosts behind them.

■ The target hosts include all desktops in Internal_Clients, Internal_Admin and Internal_Dev.

■ Due to the Intruder AutoBlock feature of the Norton firewall, everytime a scan is completed the block must be removed before attempting another scan.

Scan from	Target(s)	Tool	Ports/Shares discovered	Intrusion logged	Comments / Recommended actions
192.168.16.99	**Norton1_IDS**	**SuperScan**	**Nil**	**Yes**	
192.168.16.99	**192.168.17.0**	**SuperScan**	**Nil**	**Yes**	
192.168.16.99	**Norton1_IDS**	**Retina**	**Nil** *** OS cannot be detected.**	**Yes**	**The fact that the OS type of the firewall is successfully hidden deserves a highly positive comment.**
192.168.16.99	**192.168.17.0**	**Retina**	**Nil**	**Yes**	
192.168.16.99	**Norton1_IDS**	**NetBrute**	**Nil**	**No**	**The fact that share scanning / share access attempts are blocked but not logged is understandable, as Norton Firewall's intrusion detection and reporting mechanism is geared towards port-based attempts rather than share-based attempts.**
192.168.16.99	**192.168.17.0**	**NetBrute**	**Nil**	**No**	
192.168.16.99	**Norton1_IDS**	**Share Scanner**	**Nil**	**No**	
192.168.16.99	**192.168.17.0**	**Share Scanner**	**Nil**	**No**	
192.168.16.99	**Norton1_IDS**	**Sub_Net**	**Nil**	**Yes**	
192.168.16.99	**192.168.17.0**	**Sub_Net**	**Nil**	**Yes**	
192.168.16.99	**Norton2_IDS**	**SuperScan**	**Nil**	**Yes**	
192.168.16.99	**192.168.19.0**	**SuperScan**	**Nil**	**Yes**	

192.168.16.99	Norton2_IDS	Retina	Nil * OS cannot be detected.	Yes	The fact that the OS type of the firewall is successfully hidden deserves a highly positive comment.
192.168.16.99	192.168.19.0	Retina	Nil	Yes	
192.168.16.99	Norton2_IDS	NetBrute	Nil	Yes	
192.168.16.99	192.168.19.0	NetBrute	Nil	Yes	
192.168.16.99	Norton2_IDS	Share Scanner	Nil	Yes	
192.168.16.99	192.168.19.0	Share Scanner	Nil	Yes	
192.168.16.99	Norton2_IDS	Sub_Net	Nil	Yes	
192.168.16.99	192.168.19.0	Sub_Net	Nil	Yes	
192.168.16.99	Norton3_IDS	SuperScan	Nil	Yes	
192.168.16.99	192.168.20.0	SuperScan	Nil	Yes	
192.168.16.99	Norton3_IDS	Retina	Nil * OS cannot be detected.	Yes	The fact that the OS type of the firewall is successfully hidden deserves a highly positive comment.
192.168.16.99	192.168.20.0	Retina	Nil	Yes	
192.168.16.99	Norton3_IDS	NetBrute	Nil	Yes	

192.168.16.99	192.168.20.0	NetBrute	Nil	Yes	
192.168.16.99	Norton3_IDS	Share Scanner	Nil	Yes	
192.168.16.99	192.168.20.0	Share Scanner	Nil	Yes	
192.168.16.99	Norton3_IDS	Sub_Net	Nil	Yes	
192.168.16.99	192.168.20.0	Sub_Net	Nil	Yes	

Rulebase assessment

In Internal_Admin, create a share that allows everyone access. From Internal_Clients, attempt to access such share.	**Attempt failed. This is the desirable result.**
In Internal_Dev, create a share that allows everyone access. From Internal_Clients, attempt to access such share.	**Attempt failed. This is the desirable result.**

Other assessment methods

From a protected host, connect to an internet site that offers Java and ActiveX codes, and try to have them downloaded.	**Downloads blocked and logged.**

Remarks

It seems like the Norton Firewalls are providing excellent protection. In fact, it is the Intruder AutoBlock function that allows the firewall to reject all subsequent connection attempts coming from the blocked intruders.	**This feature may not work well when attacks are initiated with random source IP addresses. Therefore, further testing using a tool capable of random spoofing is recommended.**

Scenario Three:

> **Scenario Three: Attacker trying to tamper with the public service servers.**

```
  ┌─────────┐        ┌──────────────┐        ┌─────────┐
 (  Attacker  ) ───▶ │   FW2_B2C    │ ───▶ (  Target   )
  └─────────┘        └──────────────┘       ( Hosts at  )
                                            ( 192.168.8.0)
                                             └─────────┘
```
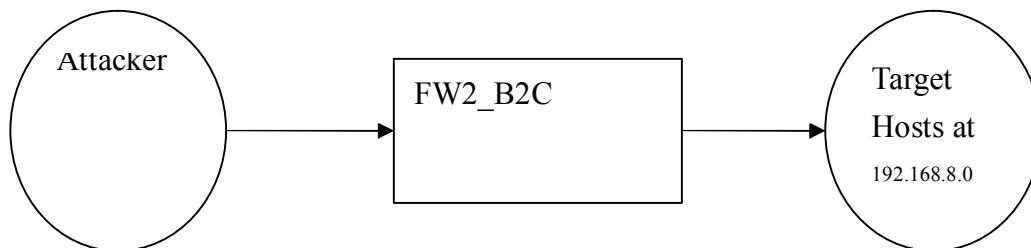
Segments involved: Core_Net (192.168.16.0), Public_Services (192.168.8.0)

Remarks:

■ Scanning will be performed against the firewall itself and against the hosts behind it.

■ The hosts include all the public service servers and the IDS within the segment.

Scan from	Target(s)	Tool	Ports/Shares discovered	Intrusion logged	Comments / Recommended actions
192.168.16.99	**FW2_B2C**	**SuperScan**	**Nil**	**Yes**	
192.168.16.99	**192.168.8.0**	**SuperScan**	**Nil**	**Yes**	
192.168.16.99	**FW2_B2C**	**Retina**	**Nil** *** OS cannot be detected.**	**Yes**	**The fact that the OS type of the firewall is successfully hidden deserves a highly positive comment.**
192.168.16.99	**192.168.8.0**	**Retina**	**All the allowed service ports.**	**Yes**	
192.168.16.99	**FW2_B2C**	**NetBrute**	**Nil**	**Yes**	
192.168.16.99	**192.168.8.0**	**NetBrute**	**Nil**	**Yes**	
192.168.16.99	**FW2_B2C**	**Share Scanner**	**Nil**	**Yes**	
192.168.16.99	**192.168.8.0**	**Share Scanner**	**Nil**	**Yes**	
192.168.16.99	**FW2_B2C**	**Sub_Net**	**Nil**	**Yes**	
192.168.16.99	**192.168.8.0**	**Sub_Net**	**Nil**	**Yes**	

Rulebase assessment

Initiate the following connections towards the Ecommerce web service server:

■   non-HTTP/HTTPS traffic from Internal_Dev

All connections failed. This is the desirable result.

- non-HTTP/HTTPS traffic from Internal_Clients.
- non-HTTP/HTTPS traffic from RAS_Net.
- HTTP/HTTPS traffic from a new unknown subnet.

Initiate the following connections towards the external email service server: ■ non-SMTP traffic from the internal server segment ■ POP3 traffic from the internal clients segment	**All connections failed. This is the desirable result.**
Initiate the following connections towards the external DNS service server: ■ non-DNS query traffic from Internal_Dev. ■ non-DNS query traffic from Internal_Clients. ■ non-DNS query traffic from RAS_Net.	**All connections failed. This is the desirable result.**
Initiate non-SMTP connections towards the internal email server from the IDS. Initiate SMTP connections towards the IDS from the internal email server. Deliberately trigger the IDS to send an alert. See if the message can reach the internal SMTP server.	**Connections succeeded. This is the desirable result.** **Connections failed. This is the desirable result.** **Message arrived at the administrator's mailbox successfully.**

Other assessment methods

NSLOOKUP – initiate a zone transfer against the DNS server behind the firewall from internal_clients. According to Microsoft's KB Article Q200525:	**The zone transfer operation fails. Such a failure is a desirable behavior. Attempt logged.**

---

[47] http://support.microsoft.com/search/preview.aspx?scid=kb;en-us;Q200525

"NSLOOKUP can be used to transfer an entire zone by using the ls command. This is useful to see all the hosts within a remote domain. The syntax for the ls command is:

ls [- a | d | t type] domain [> filename]"[47]

Scenario Four:

Scenario Four: Attacker trying to login via RAS.

Attacker
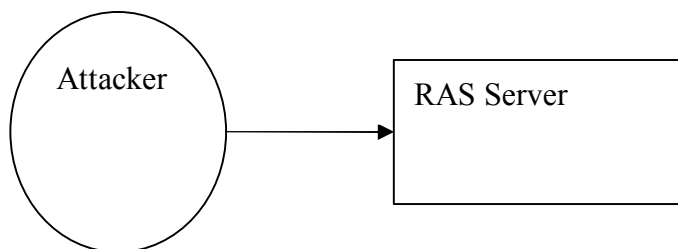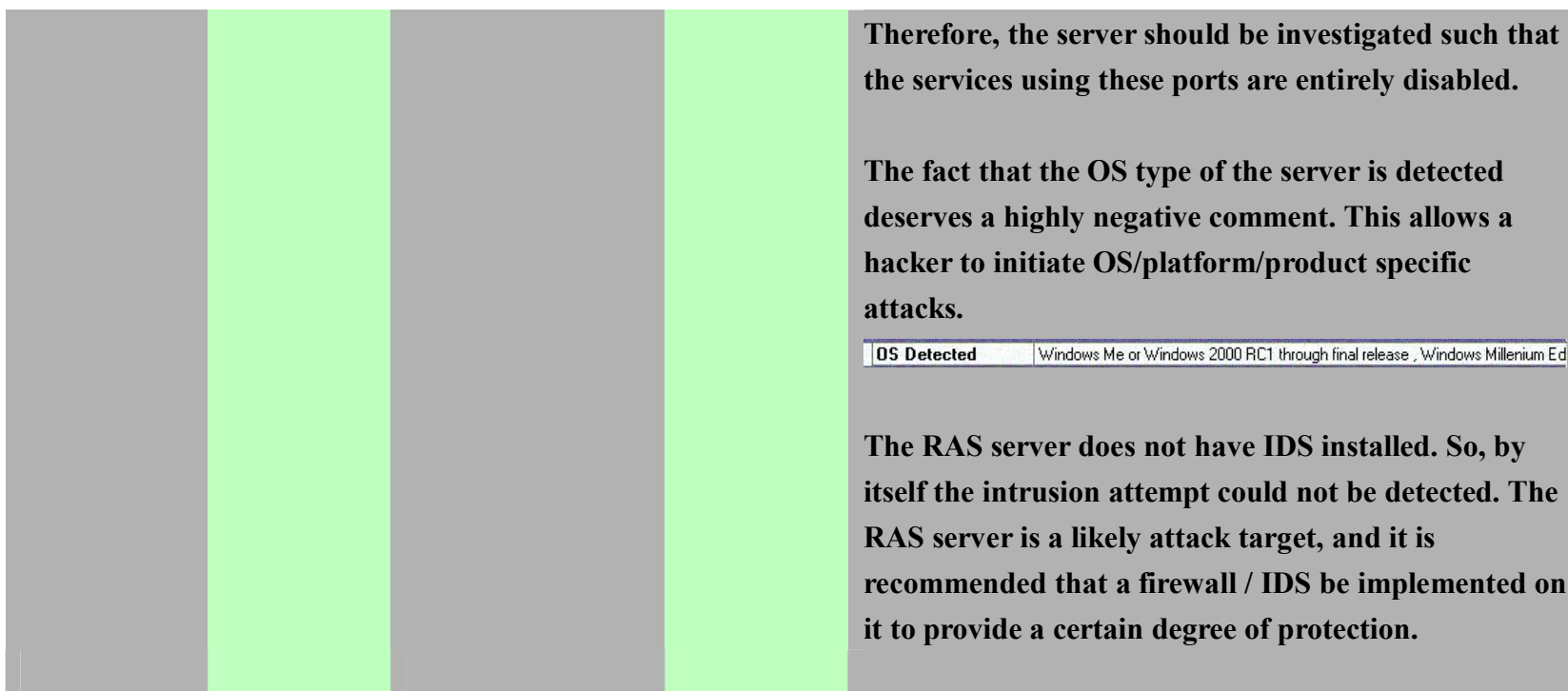
RAS Server

Remarks: This test focuses on testing whether the RAS Server can distinguish between legitimate and illegitimate login requests.

* Audit Positioning: Although this test involves dialing from the "outside" into the RAS Server, arrangement should be made so that the dialing can be performed in-house, probably using a free phone line. This minimizes the chance of having the test being monitored by a third party, as

recommended in the book "Hack Proofing your E-Commerce Site"[48].

---

[48] Published by Syngress, ISBN: 1-928994-27-X, http://www.syngress.com/catalog/sg_main.cfm?pid=1216

Scan from	Target	Tools	Ports/Shares discovered	Intrusion logged	Comments / Recommended actions
Outside	RAS_Server	SuperScan	80, 81, 82, 83	N/A	The details of the detected ports are:
Outside	RAS_Server	Retina	80, 81, 82, 83, 1032, 1080, 8080 * OS type detected.	N/A	hosts2-ns 81/tcp HOSTS2 Name Server hosts2-ns 81/udp HOSTS2 Name Server xfer 82/tcp XFER Utility xfer 82/udp XFER Utility mit-ml-dev 83/tcp MIT ML Device
Outside	RAS_Server	NetBrute	Nil	N/A	mit-ml-dev 83/udp MIT ML Device
Outside	RAS_Server	Share Scanner	Nil	N/A	1032/tcp BBN IAD
Outside	RAS_Server	Sub_Net	8080	N/A	1032/udp BBN IAD 1080/tcp Socks 1080/udp Socks 8080/tcp proxy 8080/udp proxy * TCP 8080 is subject to the Ring Zero Trojan attack. None of these ports are needed in a RAS server.

Therefore, the server should be investigated such that the services using these ports are entirely disabled.

The fact that the OS type of the server is detected deserves a highly negative comment. This allows a hacker to initiate OS/platform/product specific attacks.

OS Detected	Windows Me or Windows 2000 RC1 through final release , Windows Millenium Ed

The RAS server does not have IDS installed. So, by itself the intrusion attempt could not be detected. The RAS server is a likely attack target, and it is recommended that a firewall / IDS be implemented on it to provide a certain degree of protection.

Other assessment methods

Configure a modem dial up client to dial into the RAS server. Test the authentication mechanism and the call back security setting:

■ Try to make multiple login attempts with the wrong passwords to determine if account lockout works.

■ Try to disable caller ID and make calls from different phone numbers to see if call-back security works.

The RAS Server successfully authenticated the legitimate users and rejected the non-legitimate clients.

Although the RAS server can satisfactorily authenticate users and maintain a certain level of security, it is important to realize the points below:

- The RAS phone number should always be kept confidential.
- It is technically possible to achieve the effect of DoS against the RAS Server by keeping on repeating calls to the RAS lines. There is no way to stop this kind of attack.

Modem dial-in is always considered as a "back door" to network security. Extreme care must be made to ensure its security.

Assessment - from an "Outsider" perspective

Again, we need to first identify the possible attack routes used by the attackers and build the corresponding test scenarios. This time the attacks are originated from the outside world.

Scenario One: Attacker trying to compromise the border router.
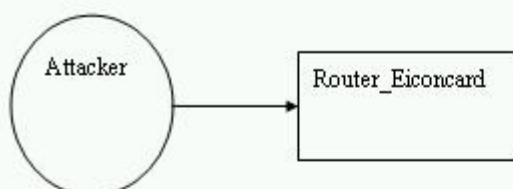
Attacker → Router_Eiconcard

Scenario Two: Attacker trying to tamper with the public service servers.

Attacker → FW1_B2C → Target Hosts at 192.148.8.0

Scenario Three: Attacker trying to pass through the VPN server to the internet network.

Attacker → W2K_VPN → Target Hosts at 192.148.14.0

Scenario Four: Attacker trying to compromise the proxy server.

Attacker → ISA_Cache → Target Hosts at 192.148.17.0 192.148.19.0 192.148.20.0

Scenario One:

┌───┐
│ **Scenario One: Attacker trying to compromise the border router.** │
│ │
└───┘

Attacker ⟶ Router_Eiconcard
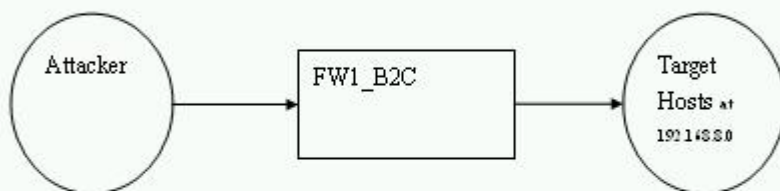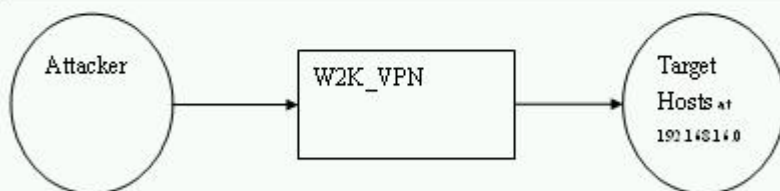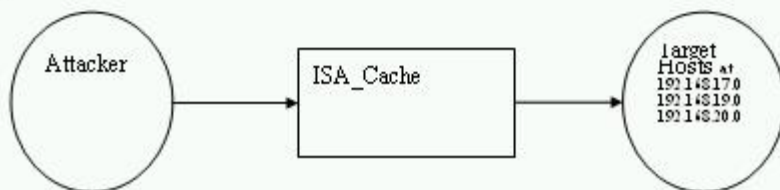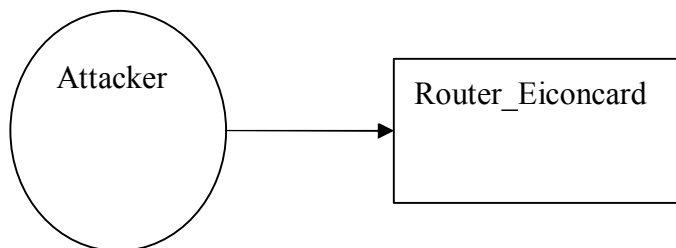
Remarks:

The router is configured with only one type of filter – filter against spoofing.

* Audit Positioning: Although this test involves connecting from the "outside", arrangement should be made so that the internet connection can be performed in-house, probably using a dial up ISP connection. This minimizes the chance of having the test being monitored by a third party, as recommended in the book "Hack Proofing your E-Commerce Site"[49].

---

[49] Published by Syngress, ISBN: 1-928994-27-X, http://www.syngress.com/catalog/sg_main.cfm?pid=1216

Scan from	Target(s)	Tool	Ports/Shares discovered	Intrusion logged	Comments / Recommended actions
Outside	Router_Eico ncard	SuperScan	Ports 7, 9, 13, 17, 19, 135	N/A	The details of these detected ports are:
Outside	Router_Eico ncard	Retina	Ports 7, 9, 13, 17, 19, 135, 1032 * OS type detected.	N/A	7/tcp Echo 7/udp Echo 9/tcp Discard 9/udp Discard 11/tcp Active Users 11/udp Active Users 13/tcp Daytime 13/udp Daytime 17/tcp Quote of the Day 17/udp Quote of the Day 19/tcp Character Generator 19/udp Character Generator 135/tcp Location Service 135/udp Location Service 1032/tcp BBN IAD 1032/udp BBN IAD The function of Router_Eiconcard is routing and

nothing else. The existence of any active port must be investigated to determine if they are relevant to the routing functions. While there is no known vulnerability on these ports that are related to the Eiconcard routing application, they should be filtered at the WAN interface if they are of no use.

The fact that the OS type of the router is detected deserves a highly negative comment. This allows a hacker to initiate OS/platform/product specific attacks. However, without a firewall service running on it, such weakness can hardly be eliminated.

Outside	**Router_Eico ncard**	**NetBrute**	**Nil**	**N/A**
Outside	**Router_Eico ncard**	**Share Scanner**	**Nil**	**N/A**
Outside	**Router_Eico ncard**	**Sub_Net**	**8080**	**N/A**

For the last row, the comment column reads:

The router does not act as a proxy. Therefore, access to this port should be filtered at the WAN interface.

* TCP 8080 is subject to the Ring Zero Trojan attack.

Other assessment methods

An attacking host with its IP address deliberately set to an "internal" address is used for making connections through the router to the systems behind it. This is done to simulate the effect of IP Spoofing.

Connections failed. This is the desirable result.

Scenario Two:

Scenario Two: Attacker trying to tamper with the public service servers.

Attacker → FW1_B2C → Target Hosts at 192.168.8.0
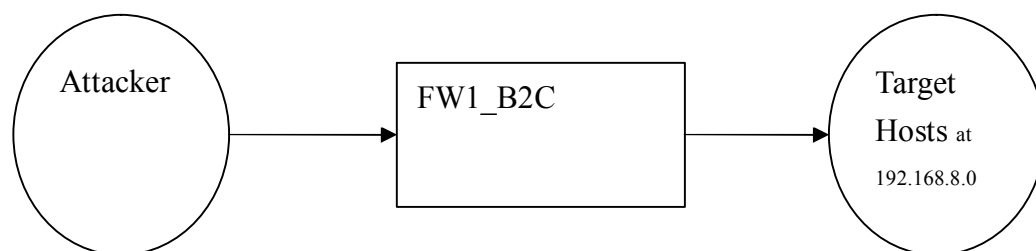
Segments involved: Outside world, Public_Services (real address 192.168.8.0 / published address 192.168.7.0)

Remarks: Apart from scanning, we perform stress testing against the web services behind the firewall to see if:

■ the firewall will break due to the high load

■ the firewall can protect the web server from this kind of attack

We do not, however, intend to measure the firewall performance in-depth.

* Audit Positioning: Although this test involves connecting from the "outside", arrangement should be made so that the internet connection can be performed in-house, probably using a dial up ISP connection. This minimizes the chance of having the test being monitored by a third party,

as recommended in the book "Hack Proofing your E-Commerce Site"[50].

Scan from	Target(s)	Tool	Ports/Shares discovered	Intrusion logged	Comments / Recommended actions
Outside	FW1_B2C	SuperScan	Nil	Yes	The fact that the OS type of the firewall is successfully hidden deserves a highly positive comment.
Outside	192.168.7.0 (published addresses)	SuperScan	Nil	Yes	
Outside	FW1_B2C	Retina	Nil * OS type cannot be detected.	Yes	
Outside	192.168.7.0 (published addresses)	Retina	Nil	Yes	
Outside	FW1_B2C	NetBrute	Nil	Yes	
Outside	192.168.7.0 (published addresses)	NetBrute	Nil	Yes	
Outside	FW1_B2C	Share Scanner	Nil	Yes	
Outside	192.168.7.0 (published addresses)	Share Scanner	Nil	Yes	

---

[50] Published by Syngress, ISBN: 1-928994-27-X, http://www.syngress.com/catalog/sg_main.cfm?pid=1216

| Outside | **FW1_B2C** | **Sub_Net** | **Nil** | **Yes** | |
| Outside | **192.168.7.0 (published addresses)** | **Sub_Net** | **Nil** | **Yes** | |

Rulebase assessment

Initiate connections towards the Ecommerce web service server via protocols OTHER THAN HTTP and SSL.	**Connections failed. This is the desirable result.**
Initiate connections towards the external Email service server via protocols OTHER THAN SMTP.	**Connections failed. This is the desirable result.**
Initiate connections towards the external DNS service server via protocols OTHER THAN DNS Query.	**Connections failed. This is the desirable result.**

Stress Testing

* Before proceeding, explicit approval must be obtained, and advanced notice must be given. These tests should be conducted only during non-peak hours.

| Web Server Stress Tool and UDP Flood – we use these tools to stress test the firewall. The goal is to determine if heavy traffic can break the firewall in between, or if the firewall will become a bottleneck. To simulate a high number of simultaneous users, we need the enterprise edition of the Web Stress Tool (which poses no user restriction). The ideal setting is to set the number of users to at least 1000. For maximum performance, run these tests from multiple machines to share the load. | **The firewall ran smoothly without trouble. Below are the results:**

First run:

Ave. Time per Request [ms]
259
514 |

First of all, a baseline is obtained by running stress tests against the web server directly without the firewall:

Baseline result:

Then, run the following test for two times:

Run Web Server Stress Tool and UDP Flood against the public address of the web server at the same time. For UDP Flood, use variable size packets directly against port 80. For Web Server Stress Tool, test against 2 URLs on the web server, with the URLs being accessed at random by each user. Run the test for 30 minutes.

Second run:

The above results show the average response time for each URL tested. Since the URLs are selected by random from a pool of 2, the first result set looks very different from the second result set. However, with a little calculation, we can conclude that these results are consistent.

First run: (259 + 514) / 2 = 386.5
Second run: (350 + 387) / 2 = 368.5

The test results clearly show that the firewall has effectively protected the web server during deadly-high traffic load.
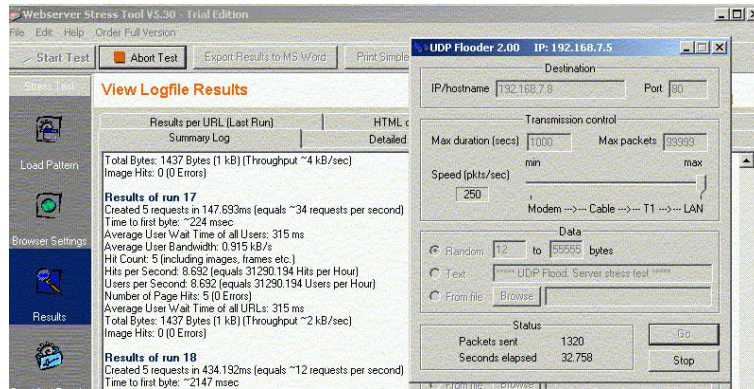
Scenario Three:

Scenario Three: Attacker trying to pass through the VPN server to the internet network.

Attacker → W2K_VPN → Target Hosts at 192.168.16.0
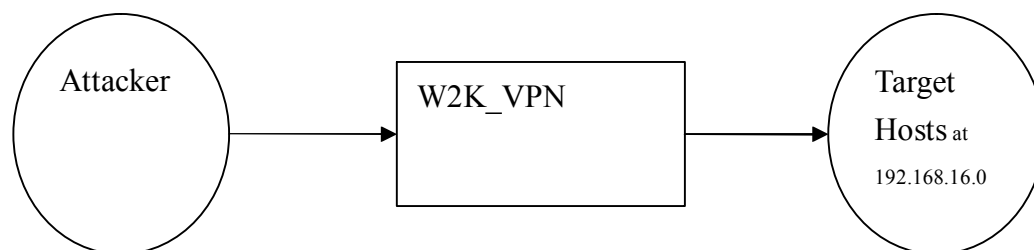
Segments involved: Outside world, Core_Net (192.168.16.0)

Remarks:

■ This test is designed to find out if non-legitimate remote clients can access the network via W2K_VPN.

■ A hosts with default Windows 2000 installation and shares opened is deliberately placed in Core_Net (behind W2K_VPN) for testing.

* Audit Positioning: Although this test involves connecting from the "outside", arrangement should be made so that the internet connection can be performed in-house, probably using a dial up ISP connection. This minimizes the chance of having the test being monitored by a third party, as recommended in the book "Hack Proofing your E-Commerce Site"[51].

---

[51] Published by Syngress, ISBN: 1-928994-27-X, http://www.syngress.com/catalog/sg_main.cfm?pid=1216

Scan from	Target(s)	Tool	Ports/Shares discovered	Intrusion logged	Comments / Recommended actions
Outside	**W2K_VPN**	**SuperScan**	**7, 9, 13, 17, 19, 135, 1032, 1080, 8080**	**N/A**	**Detail of the detected ports:**
					7/tcp Echo
Outside	192.168.16.0	**SuperScan**	**Nil**	**N/A**	**7/udp Echo**
Outside	**W2K_VPN**	Retina	**7, 9, 13, 17, 19, 135, 1032, 1723**	**N/A**	**9/tcp Discard**
					9/udp Discard
					13/tcp Daytime
			* OS type detected.		**13/udp Daytime**
					17/tcp Quote of the Day
Outside	192.168.16.0	**Retina**	**Nil**	**N/A**	**17/udp Quote of the Day**
					19/tcp Character Generator
					19/udp Character Generator
					135/tcp Location Service
					135/udp Location Service
					1080/tcp Socks
					1080/udp Socks
					1032/tcp BBN IAD
					1032/udp BBN IAD

---

[52] http://cio.cisco.com/warp/public/707/3.html

1723/tcp PPTP
8080/tcp proxy
8080/udp proxy

The function of W2K_VPN is servicing remote access VPN clients and nothing else. The existence of any active port must be investigated to determine if they are relevant to the remote access functions. While there is no known vulnerability on these ports that are related to RRAS, we recommend the consideration of filtering them (except 1723, which is required by PPTP).

Specific attention must be given to port 7, 9 and 13. According to Cisco, these ports are known as small servers that can get involved in DoS attack[52].

The fact that the OS type of the server is detected deserves a highly negative comment. This allows a hacker to initiate OS/platform/product specific attacks. However, without a firewall service running on it, such weakness can hardly be eliminated.

Outside	W2K_VPN	NetBrute	Nil	N/A	
Outside	192.168.16.0	NetBrute	Nil	N/A	
Outside	W2K_VPN	Share Scanner	Nil	N/A	
Outside	192.168.16.0	Share Scanner	Nil	N/A	
Outside	W2K_VPN	Sub_Net	8080	N/A	**Again, 8080 is not needed. It should be filtered.** *** TCP 8080 is subject to the Ring Zero Trojan attack.**
Outside	192.168.16.0	Sub_Net	Nil	N/A	

Rulebase assessment:

Set up a VPN client with an address not included in the "allowed partners/suppliers list". Try to make PPTP connections to the server.

Connection fails. Events logged in the RAS log. This is the desirable result.

Set up a VPN client with an address included in the "allowed partners/suppliers list". Try to make a non-PPTP connections to the server.

Connection fails. Events logged in the RAS log. This is the desirable result.

Scenario Four:

Scenario Four: Attacker trying to compromise the proxy server.

Attacker → ISA_Cache → Target Hosts at 192.168.17.0 192.168.19.0 192.168.20.0
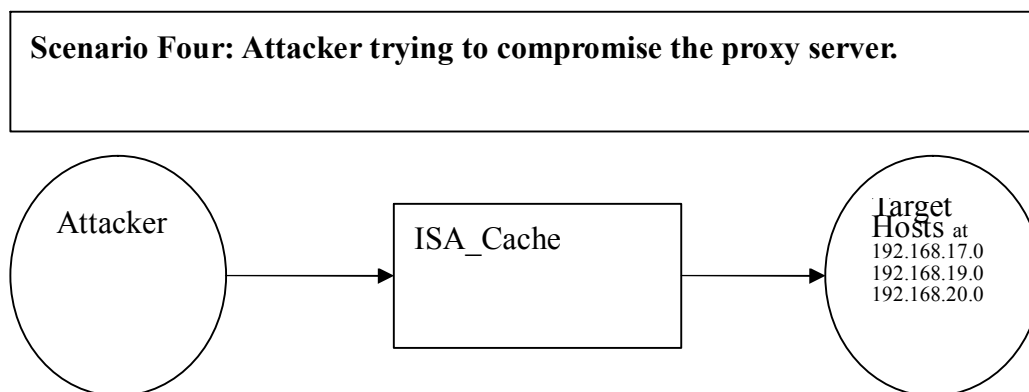
Segments involved: Outside world, Internal_Clients (192.168.17.0), Internal_Admin (192.168.19.0), Internal_Dev (192.168.20.0)

Remarks: This test attempts to find out:

- whether threats can flow through to the internal network
- whether attackers are prevented from making use of the proxy function

* Audit Positioning: Although this test involves connecting from the "outside", arrangement should be made so that the internet connection can be performed in-house, probably using a dial up ISP connection. This minimizes the chance of having the test being monitored by a third party, as recommended in the book "Hack Proofing your E-Commerce Site"[53].

---

[53] Published by Syngress, ISBN: 1-928994-27-X, http://www.syngress.com/catalog/sg_main.cfm?pid=1216

Scan from	Target(s)	Tool	Ports/Shares discovered	Intrusion logged	Comments / Recommended actions
Outside	ISA_Cache	SuperScan	Nil	Yes	The fact that the OS type of the firewall is successfully hidden deserves a highly positive comment.
Outside	192.168.17.0	SuperScan	Nil	Yes	
Outside	192.168.19.0	SuperScan	Nil	Yes	
Outside	192.168.20.0	SuperScan	Nil	Yes	ISA Server's intrusion detection feature is essential to the blocking of port scanning attempts. The result here shows that this feature DOES work smoothly.
Outside	ISA_Cache	Retina	Nil * OS type cannot be detected.	Yes	
Outside	192.168.17.0	Retina	Nil	Yes	
Outside	192.168.19.0	Retina	Nil	Yes	
Outside	192.168.20.0	Retina	Nil	Yes	
Outside	ISA_Cache	NetBrute	Nil	Yes	
Outside	192.168.17.0	NetBrute	Nil	Yes	
Outside	192.168.19.0	NetBrute	Nil	Yes	
Outside	192.168.20.0	NetBrute	Nil	Yes	
Outside	ISA_Cache	Share Scanner	Nil	Yes	
Outside	192.168.17.0	Share	Nil	Yes	

Outside	192.168.19.0	**Scanner Share Scanner**	**Nil**	**Yes**
Outside	192.168.20.0	**Share Scanner**	**Nil**	**Yes**
Outside	**ISA_Cache**	**Sub_Net**	**Nil**	**Yes**
Outside	192.168.17.0	**Sub_Net**	**Nil**	**Yes**
Outside	192.168.19.0	**Sub_Net**	**Nil**	**Yes**
Outside	192.168.20.0	**Sub_Net**	**Nil**	**Yes**

Rulebase assessment:

Set up IIS to run on a test target host behind ISA_Cache, then try to use web browser to connect to it from the outside.	**Fail to access the site. This is the desirable result.**
Configure an internal client with an IP address that belongs to a non-valid subnet to connect to ISA_Cache's port 8080 for web browsing.	**Connection failed. This is the desirable result.**
From the outside, connect to ISA_Cache's port 8080 for web browsing.	**Connection failed. This is the desirable result.**

Administrative Security Assessment

For every firewall and router in use, determine the following:

- Are they physically secured?
- Does local login access require (as always) valid credentials to be supplied?
- Are the default login names (such as administrator) removed?
- What is the minimum required length of the login password?
- When the local console is idle for 1 minute, will any password protected screensaver come up?
- How many different administrators are allowed to login? Do they have separate sets of credentials?
- Is there any established procedure for controlling the changes of rules or other settings on the firewall?
- Who have access to the local file systems where the firewall products / log files reside? Are the security policy files / log files adequately protected by the file system ACLs?

Fault Tolerance Assessment

For every firewall and router in use, determine the following:

- Are the log files backed up regularly? (Check the backup log sheet)
- Are the backup tapes that hold the logs probably stored?
- Is the UPS running? Does it connect well with the corresponding OS service? How about the battery level?
- Is disk mirroring fully functional?
- What is the current disk space utilization? (Out of disk space is the primary reason for Windows based machine to crash)
- Are there any difference in settings between the production system and the standby system? (Any change in settings made to the production system must be replicated to the standby system and to the backup disk image)

Audit Report

Audit of the GIAC network security architecture was performed from 4th April to 8th April, 2002. During this audit, the following areas were assessed and reviewed:

- ◊ Existing security policies and procedures
- ◊ Logical and physical security measures
- ◊ Security devices configurations
- ◊ Rulebase implementations and policies compliance
- ◊ Administrative and change control procedures

We conclude that the GIAC security architecture is successful in securing the network:

- The firewall systems are working as expected without major problems. On top of this, the layered defense architecture makes it possible to mitigate any serious threat.
- Documentation, change control and other administrative procedures are in place and are properly followed.
- During the technical assessment phrases, most vulnerabilities found are minor and are related to the non-firewall devices, including the Windows 2000 based border router, the VPN server and the RAS server.
- In terms of performance, fault tolerance and remote access security, room for further improvement does exist.

Below is a list of recommendations:

Recommendation One

Although there are two separate links for use by GIAC, the B2B stream is sharing bandwidth with the INET stream without any bandwidth coordination mechanism in place. A QoS solution such as the Check Point FloodGate-1 software should be considered at Router_Eiconcard:

"FloodGate-1® is a policy-based, Quality of Service (QoS) solution for VPNs, private WANs and Internet links. It optimizes network performance by assigning priority to

business critical applications and end-users. FloodGate-1 can be deployed with VPN-1®/FireWall-1® or standalone." (from www.checkpoint.com[54])

Or, if cost is an issue, partial bandwidth control can be exercised via ISA Server's built-in Bandwidth Rules. KB article 302527 explains in detail how to configure this feature[55]. With this feature enabled, bandwidth usage on the INET stream can be controlled.

Recommendation Two

Fault tolerance using standby systems is not an optimal solution. First of all, switching to the standby system involves certain downtime. Secondly, keeping the production system and the standby system in-sync is a time consuming manual job. Therefore, advanced fault tolerance solution should be considered. Both NT4 and Windows 2000 Advanced Server edition support clustering, a popular strategy for connecting multiple computers together in such a way that they behave as a single unit[56].

Recommendation Three

There is no fault tolerance provided for the WAN links. Technology such as DDR should be considered. With DDR (Dial-on-Demand Routing), the backup connection only becomes active when the primary links fail[57].

Recommendation Four

Regardless of what firewall technology is in use, traffic is allowed to flow to the web server via port 80 and 443. The scripts on the web server are potential sources of various security threats[58]. It is recommended that an audit on all the server scripts be performed.

---

[54] http://www.checkpoint.com/products/performance/floodgate-1.html
[55] http://support.microsoft.com/view/tn.asp?kb=302527
[56] http://www.webopedia.com/TERM/c/clustering.html
[57] http://www.webopedia.com/TERM/D/DDR.html
[58] "Programming Secure Scripts", Hack Proofing Your E-commerce Site, ISBN: 1-928994-27-X, http://www.syngress.com/catalog/sg_main.cfm?pid=1216

Recommendation Five

It is recommended that an audit be performed on the partner/supplier sites. Since these partners and suppliers are granted VPN access, any problem on their ends can produce negative impacts on GIAC network.

Recommendation Six

It is recommended that smart card authentication be deployed for RAS. This introduces an additional layer of security: if a staff is currently logged on locally in the office using his/her smart card, no one else at home can dial in.

Recommendation Seven

As said before, the non-firewall devices have quite a few minor vulnerabilities detected. Therefore, it is recommended that either firewall/IDS services be deployed on these computers, or have IP filters configured on the computers' interfaces to block access to the detected ports.

Assignment 4

Design under fire

Attack Target

Vincent Berk's design at http://www.sans.org/y2k/practical/Vince_Berk_GCFW.zip.
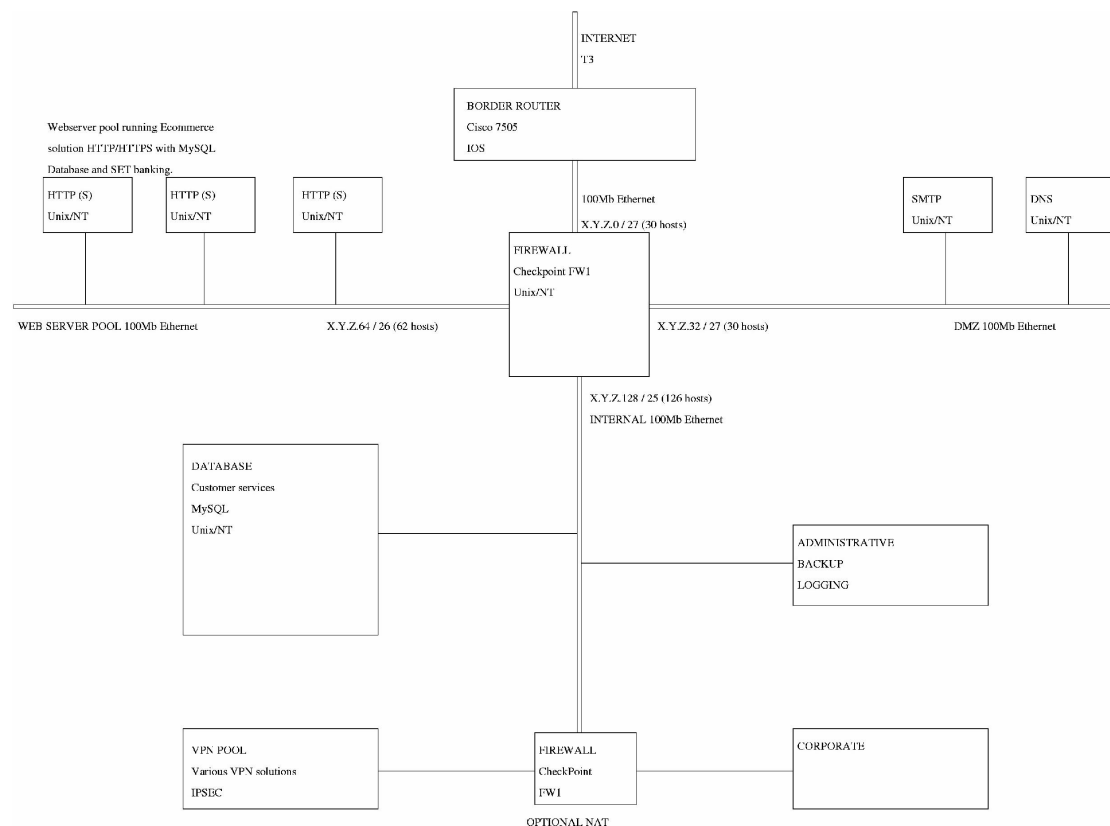
The reasons I choose this design as my attack target are:

◊ It uses Check Point FW-1. FW-1 has quite a number of vulnerabilities publicly available, thus giving me more "attack opportunities". I assume that the version in use is the popular 4.x series.

◊ It does not use specific content filtering solution / anti-virus solution, thus providing room for content/virus related attacks.

Firewall Attack

Information Gathering:

Visit the target GIAC web site. Study it thoroughly. Know what business it is in. Know what functions the site is providing. From the "site visit", we can tell what application protocols are allowed (such as HTTP, HTTPS, FTP, SMTP…etc.), and can make an educated guess on the rulebase configuration.

Run NSLOOKUP against GIAC. A typical setup used by many ecommerce sites is to have a secondary DNS server running offsite somewhere (mostly likely in the ISP's premise). NSLOOKUP tells us what DNS servers are used by GIAC. If one DNS server is hosted offsite, zone transfer traffic has to be allowed between the onsite DNS and the offsite DNS. This opens up a potential security hole.

Collect information about the firewall. Although the architecture map we have on hand shows clearly that FW-1 is the primary firewall in use, this might have been changed by the time we plan the attack.

Angela Orebaugh in her GCFW practical[59] suggests that we detect FW-1 by scanning its default TCP ports at 256, 257, and 258 using nmap (nmap –n –vv –P0 –p256,257,258 X.Y.Z.1-.254), or by running traceroute against GIAC's site (#traceroute www.giacfortunes.com). I personally tried using Retina (which is based on nmap technology[60]) to scan a FW-1 installation, and found that its OS type can be detected only if the stealth rule is disabled.

Too much scanning may trigger any hidden IDS and block our subsequent intrusion attempts!

Attacking – the port 259 route:

This attack allows us to bypass FW-1 and reach the internal hosts behind it.

---

[59] http://www.giac.org/practical/Angela_Orebaugh_GCFW.zip
[60] http://www.eeye.com/html/Products/Retina/index.html

Since we just talked about the default ports, one thing we can try is to explore vulnerabilities related to FW-1's ports. A search on CERT returns one such vulnerability. This vulnerability involves port 259 and is related to FW-1's RDP protocol:

"By adding a faked RDP header to typical UDP traffic, any content can be passed to port 259 on any host on either side of the device." [61]

So, how do we launch an attack based on this information? The best thing to do is to look at the "Proof of concept code" available at http://www.inside-security.de/fw1_rdp_poc.html. The source code is available in C language. By compiling our own attack program using these codes, such attack can be launched. Keep in mind though, that this vulnerability is found only on FW-1 version 4.1. There is no evidence that identical vulnerability exists in version 4.0.

For GIAC administrator to work on this issue, it is suggested that the following workarounds supplied by insideSECURITY be followed:

"

Comment line 2646 of base.def (accept_fw1_rdp;)
Deactivate implied rules in the Check Point policy editor (and build your own rules for management connections).
Block UDP traffic to port 259 on your perimeter router.
"[62]

Attacking – the Trojan route:

This attack allows us to take control of FW-1.

We already know from our "web site visit" what protocols are allowed in GIAC's security architecture. Remember we talked about secondary DNS server and zone transfer? FW-1 4.x's default policy setting does allow traffic that heads towards TCP port 53 to pass. Since many administrators simply leave this option as-is, what we can do then is to use NSLOOKUP or any other mean to initiate a zone transfer against the

---

[61] http://www.kb.cert.org/vuls/id/310295
[62] http://issrv1.inside-security.de/fw1_rdp.html

DNS server through the firewall. If the result is positive, we can structure an attack based on port 53 related vulnerabilities.

One possible attack option is to use Trojan horse. According to DOShelp, TCP port 53 is a popular target of Trojan horse attack[63]. A tool that can be used for this attack is Back Orifice.

Back Orifice is, in essence, a remote administration tool. According to PCHelp:

"It gives "system admin" type privileges to a remote user by way of the computer's Internet link. What does this mean? It means that if Back Orifice is running in your computer, a remote operator anywhere on the global Internet can gain access and do almost anything you can do on your computer -- and some things you can't do -- all without any outward indication of his presence.

Back Orifice can arrive disguised as a component of practically any software installation. It can be attached to other files or programs or run on its own. It must be run, by itself or by another application. It then installs itself in seconds, typically erases the original, then may run a specified program. To the user installing an "infected" application, it will appear that all went normally. But from that moment forward, your system offers easy and comprehensive access anytime it is connected to the Internet."[64]

With this tool, we can gain control of the targeted FW-1 installation. For GIAC to work against this risk, couple of things can be done:

■ Disable the default port 53 option.
■ Setup a rule that allow zone transfer only between the off-site DNS server and the on-site one. Block all other zone transfer requests.
■ Install BODetect[65] (a product specifically designed for detecting Back Orifice attacks) on the firewall.

---

63 http://www.doshelp.com/trojanports.htm
64 http://www.nwinternet.com/~pchelp/bo/bo.html
65 http://www.cbsoftsolutions.com/Products/products.htm

Attacking – the IP Fragment route:

This attack allows us to bog down FW-1.

Check Point has admitted that an IP fragment related vulnerability exists in FW-1 4.0 and 4.1. According to Check Point:

"It has been determined that a stream of large IP fragments can cause the FireWall-1 code that logs the fragmentation event to consume most available host system CPU cycles. It should be noted that no unauthorized access, information leakage, or fragment passing occurs. …. For security reasons (e.g., overlay attacks) FireWall-1 reassembles all IP fragments of a datagram prior to inspection against the security policy. After reassembly, the packet is processed by the FireWall-1 Stateful Inspection engine, and if allowed by the security policy to proceed, the packet is refragmented and forwarded. To identify and audit attacks such as Ping of Death, Check Point added a mechanism to FireWall-1 - outside of its standard logging capability - to log certain events that occur during theFireWall-1 virtual reassembly process. This fragmentation logging takes place on the gateway itself and not on the management station (relevant for distributed management deployments)."[66]

To be able to launch this attack, we need a tool capable of manipulating the ICMP packet size. Hping[67] is an ideal tool for this purpose, although it runs only on Linux and Unix. If the attack is to be launched from a Windows based machine, SMURF 2K/XP is recommended.

SMURF 2K/XP, as described by its author at theRealCoders, allows us to freely configure the following options:

"

Packets:	*Number of packets to send.*
Source:	*This is the address, the packets get labeled to 'come from'. If an internet address can't resolved, you will see a message. If this address*

---

[66] http://www.checkpoint.com/techsupport/alerts/ipfrag_dos.html
[67] http://www.hping.org/

	is changed to another one than your's, no packets get back.
Dest:	*Is the destination address, the packets should go to. If you want to ping some host, type in the address right here.*
Trace:	*The route will traced to the host. All router to the destination are found by the yellow time expired messages.*
TTL:	*This is a protection field. Its sais, how much router the packet may pass, before it dies. Max. 255 router.*
Size:	*The whole packet size, in byte. This includes the ip and the icmp protocol header. The actually transfered data is the packet size - 28 byte. But each icmp packet is timestamped by 8 byte, so the min. size is 36 byte.*
Delay:	*Delay in milliseconds between single packet sending. To send 4 packets per second (1000 milliseconds), use 1000/4 = 250 milliseconds.*
IN/OUT:	*Shows you the icmp traffic in kilobyte per seconds leaving (OUT) and receiving (IN) your host.*
[START][STOP]:	*Start or Stop the packet sending.*

"68

For the GIAC administrator to address this issue, the best thing to do is to apply the latest service pack. According to Check Point, the new kernel binaries that fix this problem have been released in Service Pack 2 of FireWall-1 version 4.1 and as a Service Pack 6 Hot Fix for FireWall-1 version 4.0 users. As of the time of this writing, newer versions of these service packs are already available.

---

[68] http://home.t-online.de/home/theRealCoders/smurf/index.html

DoS attack

The DoS attack that I will use is a Smurf attack. According to Symantec, Smurf attack is a form of DoS that uses ping:

"In the case of a Smurf DoS attack, the ping's packet return IP address is forged with the IP of the targeted machine. The ping is issued to the entire IP broadcast address. This causes every machine to respond to the bogus ping packets and reply to the targeted machine, which floods it. This is called a Smurf attack because the DoS tool used to perform the attack is called Smurf."[69]

As described by pentics.net,

"There are two parties who are hurt by this attack... the intermediary (broadcast) devices--let's call them "amplifiers", and the spoofed address target, or the "victim". The victim is the target of a large amount of traffic that the amplifiers generate."[70]

Since we have 50 compromised DSL systems at our disposal, an attack of a reasonable strength can be launched. The role of these compromised systems will be discussed shortly.

The Amplifiers

Who can act as amplifier?

Basically, any network with routers accepting IP-directed broadcast and hosts accepting ICMP packets can be used as amplifiers.

How do we locate these amplifiers?

---

[69] http://www.symantec.com/avcenter/venc/data/smurf.dos.attack.html
[70] http://www.pentics.net/denial-of-service/white-papers/smurf.cgi

In theory, we can ping around the internet to find out who can be used as amplifiers. This is, however, extremely time consuming. Also, the degree of damage produced by individual systems is highly limited. For launching attack of massive scale, the ideal amplifier candidates are networks that have IP-directed broadcast capable routers at the border and numerous clients in the internal network.

In response to the threats posed by this kind of attack, a project known as Smurf Amplifier Registry (SAR) has been launched. According to the official SAR page,

"The SAR is a tool for Internet administrators being attacked by or implicated in smurf attacks, or those who wish to take precautions. ... The SAR lets you probe Internet connected IP networks to see whether or not they are configured in a way that will allow perpetrators to use them for smurf amplification. Probing can be done interactively or in bulk. In interactive mode the SAR will probe a network, find the number of duplicates returned, and save this information in a database. If, and only if, the probed network returns 1 or more duplicate packets, it is marked as "broken". Upon gaining knowledge of a broken network, the SAR will automatically obtain information about the network and notify the relevant people of this."[71]

SAR appears to be a tool against smurf attack. However, we can take advantage of its probing feature to locate networks that are still vulnerable, and then make use of them.

Using SAR:

We can use SAR in the following ways:

1, Use it to probe a potential amplifier network:

---

[71]   http://www.powertech.no/smurf/

2, Retrieve and use the list of existing amplifiers:

Dump the Smurf Amplifier Registry in verbose text, dense text or cisco acl format.

網址(D) http://www.powertech.no/smurf/list.cgi?format=dense

```
209.39.145.255/32     1     0   2000-11-01 22:16   not-analyzed
209.39.150.0/24       7     0   2000-10-07 17:20   not-analyzed
209.39.150.255/32     4     0   2000-11-01 22:17   not-analyzed
209.39.153.0/32       1     0   2000-11-01 22:17   not-analyzed
209.39.153.255/32     1     0   2000-11-01 22:17   not-analyzed
209.39.208.0/32       1     0   2000-11-01 22:18   not-analyzed
209.39.208.255/32     1     0   2000-11-01 22:18   not-analyzed
209.39.251.0/32       1     0   2000-11-01 22:19   not-analyzed
209.39.251.255/32     1     0   2000-11-01 22:20   not-analyzed
209.39.253.0/32       1     0   2000-11-01 22:20   not-analyzed
209.39.253.255/32     1     0   2000-11-01 22:20   not-analyzed
209.40.22.0/24        2     0   2000-08-29 14:40   not-analyzed
209.40.22.0/32        2     0   2000-10-13 08:40   not-analyzed
209.40.22.255/32      2     0   2000-10-13 08:39   not-analyzed
209.40.64.255/32      1     0   2000-10-13 08:39   not-analyzed
209.40.67.0/32        1     0   2000-10-13 08:37   not-analyzed
209.40.67.255/32      2     0   2000-10-13 08:37   not-analyzed
209.40.68.0/24        2     0   2000-08-30 20:33   not-analyzed
209.40.68.0/32        1     0   2000-10-13 08:37   not-analyzed
209.40.68.255/32      2     0   2000-10-13 08:36   not-analyzed
209.41.192.0/32       1     0   2000-11-01 22:31   not-analyzed
209.41.192.255/32     1     0   2000-11-01 22:32   not-analyzed
209.41.197.0/24       2     0   2000-12-26 12:02   not-analyzed
209.41.197.0/32       2     0   2000-11-01 22:32   not-analyzed
```

Tools for the Attack

What tools should we use to launch the attack?

Below is a table of tools extracted from DeokJo Jeon's article "Understanding DDOS Attack, Tools and Free Anti-tools"[72]:

Tools	Flooding or Attack Methods
Trin00	UDP

---

[72] http://rr.sans.org/threats/understanding_ddos.php

Tribe Flood Network	UDP, ICMP, SYN. Smurf
Stacheldracht and variants	UDP, ICMP, SYN. Smurf
TFN 2K	UDP, ICMP, SYN. Smurf
Shaft	UDP, ICMP, SYN. combo
Mstream	Stream (ACK)
Trinity, Trinity V3	UDP, SYN, RST, Random Flag, ACK, Fragment, ...

Of the above tools, TFN and its variances seem to be the most popular choices. An article provided by the University of Chicago describes TFN in detail:

"Tribal Flood Network is similar to trin00 in it's general design, though there is no Windows version of it. ... Communication between the clients and daemons is done via ICMP Echo Replies. This means that the traffic looks almost identical to standard pings. It's hard to locate without looking at the contents of the packet and impossible to block at a firewall without blocking outgoing pings. The commands are hidden inside the id field of the ICMP packet... Newer versions of TFN allow for encryption of both the iplist file, the list of masters, and the data portion of the ICMP packets."[73]

So, as long as we have ICMP connectivity with the amplifiers and that the TFN daemons are running on them, we can launch an attack easily!

Using TFN:

How to use TFN?

First of all, we need to understand how TFN works. According to David Dittrich,

"TFN is made up of client and daemon programs, which implement a distributed network denial of service tool capable of waging ICMP flood, SYN flood, UDP flood,

---

[73] http://security.uchicago.edu/seminars/DDoS/tfn.shtml

and Smurf style attacks, as well as providing an "on demand" root shell bound to a TCP port. ...

The network: attacker(s)-->client(s)-->daemon(s)-->victim(s) ...

The attacker(s) control one or more clients, each of which can control many daemons. The daemons are all instructed to coordinate a packet based attack against one or more victim systems by the client."[74]

So, ideally, we ourselves should act as the attackers who control the clients at the compromised systems to direct daemons running on the amplifiers.

Below is the syntax of the original TFN:

[tribe flood network]   (c) 1999 by Mixter

usage: ./tfn   [ip] [port]
            contains a list of numerical hosts that are ready to flood
                -1 for spoofmask type (specify 0-3), -2 for packet size,
                        is 0 for stop/status, 1 for udp, 2 for syn, 3 for icmp,
                        4 to bind a rootshell (specify port)
                        5 to smurf, first ip is target, further ips are broadcasts
[ip]   target ip[s], separated by @ if more than one
[port]   must be given for a syn flood, 0 = RANDOM

The problem we have here is, TFN works well on most Linux and Unix flavors (such as Solaris and Redhat), but not on Windows! In fact, the Wintel version cannot be located (we don't even know if it exists). If the compromised systems are Windows-based, we may have to exclude them in our plan, or use another tool instead.

A Simpler Attack

Instead of using TFN, a simpler way to launch smurf attack is possible. Follow the

---

[74] http://staff.washington.edu/dittrich/misc/tfn.analysis

steps below:

1. Write a simple program that allows us to set the number of ping attempts and the use of spoofed source address. Make sure that this small program works well on the 50 compromised systems. If it is quite certain that all these compromised hosts (as well as our own host) are Windows based, we can simply use SMURF 2K/XP instead of writing our own.
2. Set the source address to the victim's IP.
3. Upload this program to the 50 compromised systems.
4. Have them ping each others repeatedly, or have them ping the SAR list of amplifiers.

Against Smurf Attack

Cisco suggests the following ways to protect a network against DoS and Smurf attacks:

"

Use the ip verify unicast reverse-path interface command on the input interface on the router at the upstream end of the connection.
Filter all RFC1918 address space using access control lists.
Apply ingress and egress filtering (see RFC 2267) using ACL.
Use CAR to rate limit ICMP packets.
"75

Although these suggestions were prepared with Cisco gears in mind, other router vendors do offer their own versions of these strategies. The point I am trying to make here is, such attacks should be stopped at or before the router. Do NOT let them reach the firewall. The firewall is busy at inspecting too many things already.

A more straight forward approach is to disallow ICMP entirely at the border router. That means, no ICMP going in and out of the network. By doing this, devices behind the border router are from free from such attack. However, internal users will not be able to ping the outside world anymore (no more ping forever). Well, there are always

---

[75] http://www.cisco.com/warp/public/707/newsflash.html

tradeoffs in life.

Still, the above approach does not solve the problem of traffic congestion. The link is still flooded with ICMP packets, and the border router has to be busy dropping every one of them. An even better way of handling such attack is to make arrangement with the ISP so that no ICMP packets are ever allowed to flow to the border router via the WAN link. This way the burden is shifted to the ISP. Whether or not this is possible is solely a matter of negotiation.

Compromising Internal Systems

When I review the different posted practical assignments, I found that most security architectures (including the one under fire here) are targeted towards protecting the servers (web servers in particular) with little emphasis on protecting the end users. Imagine the following scenarios:

Scenario 1: John downloaded a file from the internet. When he runs it, the program quickly erases every document files on his drive and at the same time sends out broadcasts to halt his local segment.

Scenario 2: Mary received a word file which comes with Macro virus via email. Upon opening the file, the virus gets triggered and eventually changes all the numbers inside Mary's Financial Statements file to random values.

The attacks in the above scenarios are possible with junior level programming skill. The steps to take are described below:

Step 1: Research the target.

By visiting GIAC's web site, we can find out what business GIAC is in. GIAC is making fortune cookies and is selling them worldwide through many different channels. We may locate different contact email addresses. We may even retrieve a list of GIAC's suppliers and partners.

Step 2: Attack!

Via the email route:
Program a macro virus. Attach it to a Word file. Mark this file as a business information related file. Send it to the contact people in GIAC, with a sender address of anyone of its suppliers and partners. Chances are that the office staffs will open any file originated from their "trusted partners".

Via the non-email route:

If GIAC has an anti-virus solution running, the email attachment may be stripped before reaching the end users. To work around this, we can setup a FTP location somewhere on the internet to host the file. Then, send an email to the contact people in GIAC with no attachment. In the email, tell them that we represent a supplier with good deals for them. Ask them to log on to our FTP and download the "catalog" file.

Fork Bombs and Viruses

Above are just examples of how we can "by-pass" the under-fired security architecture. The "files" we use can be a macro virus, a fork bomb or anything else.

According to Rohit Singh, Fork Bombs are:

"… programs or shell scripts which (either intentionally or accidentally) create new processes repeatedly (using the fork() system call.) New processes are created so fast that within no time the process table gets filled up and the system comes to a grinding halt. No other process can then be started, not even 'ps' to see who triggered that fork bomb! Killing that fork bomb means yet another process, and that's exactly what is scarce! A fork bomb might mean pressing the big Red button!"[76]

According to the Word Macro Virus FAQ, a Word Macro Virus:

*"… is a macro (list of instructions) or template file (usually with the .DOT extension) which masquerades as legitimate MS WORD documents (usually with the extension *.DOC). An infected *.DOC file, doesn't look any different to the average PC user, as it can still contain a normal document. The difference is that this document is really just a template or macro file, with instructions to replicate, and possibly cause damage. MS WORD will interpret the *.DOT macro/template file regardless of extension, as a template file. This allows for it being passed off as a legitimate document (*.DOC) This FAQ takes the position that a document is meant to be DATA, and a MACRO is at least partially executable CODE. When a document has been infected, it has been merged with executable code in a multi-part file, part data/part*

---

[76] http://rexgrep.tripod.com/rexfbdmain.htm

executable. This tends to be hidden from the user, who expects a document to be data that is READ, and not some combination of DATA and executable code designed to be executed, often against the will of the user, to wreck havok."[77]

The reasons why macro viruses are dangerous, as described by the Word Macro Virus FAQ, are:

- These viruses tend to infect the global macros, which in turn affect the entire Word Environment.
- These viruses do REPLICATE to any Microsoft Windows environment that runs a compatible copy of Word.

Counter Measures

So, what should be implemented in this under-fired GIAC architecture to tackle these threats?

1,
Install Anti-Virus solution as supplement to the email server. Although client level AV products are technically sufficient, centralized virus detection and cleaning on the email server is preferred.

For protecting the Windows based email servers, consider the following AV solutions:

eScan:
"eScan is an 'enterprise-wide' Anti-Virus software that not only scans your local/network drives but also TCP/IP Traffic* for viruses and cleans them on a "real-time" basis using the revolutionary MicroWorld Winsock Layer (MWL) technology. eScan is always working unobtrusively in the background, protecting the computer and the Network from viruses and worms all the time."[78]

MailScan:

---

[77] http://www.bocklabs.wisc.edu/~janda/macro_faq.html#WM01
[78] http://www.techarts.com/products/escan/default.asp

"MailScan is world's first 'Real-Time' Content Security Software that performs content filtering and virus scanning to offer complete and secure messaging solution for the e-business. MailScan has been designed to provide extensive security on a "Real-Time" basis against viruses and e-mails carrying harmful content. It deals with these threats before they arrive on the network, in the same way that a firewall controls user access."[79]

Alternatively, email virus filtering can be performed at the firewall. EliaShim has announced an Anti-Virus plug-in for FireWall-1. More information is available at http://www.checkpoint.com/press/partners/1997/eliashim9702.html

2,

A content filtering solution. Any content from the internet should be filtered. Checkpoint FW-1 supports CVP, which enables different firewall systems to share a common content validation server[80]. One example of such content validation server is EliaShim's eSafe:

"eSafe provides proactive, multi-tiered Internet Content Security from the gateway to the desktop, protecting the entire enterprise from: malicious code that destroys or steals digital assets, inappropriate and nonproductive material, the misuse of company resources, and Internet-borne content."[81]

3,

User education. The GIAC fellows have to get their users educated on internet security. Most attacks are not possible without the unintentional helps from the careless users!

---

[79] http://www.techarts.com/products/mailscan/default.asp
[80] http://www.webopedia.com/TERM/C/Content_Vectoring_Protocol.html
[81] http://www.eliashim.com/esafe/default.asp?cf=tl

List of References

(in alphabetical order)

Hack Proofing Your E-commerce Site, ISBN: 1-928994-27-X,

http://www.syngress.com/catalog/sg_main.cfm?pid=1216

http://cio.cisco.com/warp/public/707/3.html

http://home.t-online.de/home/theRealCoders/smurf/index.html

http://issrv1.inside-security.de/fw1_rdp.html

http://online.securityfocus.com/cgi-bin/vulns.pl

http://rr.sans.org/threats/understanding_ddos.php

http://screamer.mobrien.com/Manuals/MPRM_group/security.htm

http://screamer.mobrien.com/Manuals/MPRM_group/security.htm

http://secinf.net/info/nt/ntbastion/

http://support.microsoft.com/default.aspx?scid=kb;EN-US;q143475

http://support.microsoft.com/default.aspx?scid=kb;EN-US;q161990

http://support.microsoft.com/search/preview.aspx?scid=kb;en-us;Q200525

http://support.microsoft.com/view/tn.asp?kb=302527

http://web-server-tools.com/WebStress/webstress.htm

http://www.amazon.com/exec/obidos/ASIN/0735613885/qid=1018719524/sr=1-1/ref=sr_1_1/104-9557570-0347903

http://www.amazon.com/exec/obidos/ASIN/0735613885/qid=1018719524/sr=1-1/ref=sr_1_1/104-9557570-0347903

http://www.amazon.com/exec/obidos/ASIN/1572318058/qid=1018718363/sr=1-1/ref=sr_1_1/104-9557570-0347903

http://www.cbsoftsolutions.com/Products/products.htm

http://www.cert.org/tech_tips/win_configuration_guidelines.html

http://www.checkpoint.com/products/performance/floodgate-1.html

http://www.checkpoint.com/techsupport/alerts/ipfrag_dos.html

http://www.deerfield.com/products/mdaemon/

http://www.deerfield.com/products/visnetic_firewall/

http://www.doshelp.com/trojanports.htm

http://www.doshelp.com/trojanports.htm

http://www.eeye.com/html/Products/Retina/index.html

http://www.eicon.com/worldwide/products/WAN/s92.htm

http://www.enteract.com/~lspitz/rules.html

http://www.foundstone.com/knowledge/proddesc/superscan.html

http://www.foundstone.com/knowledge/proddesc/udpflood.html

http://www.giac.org/practical/Angela_Orebaugh_GCFW.zip

http://www.hping.org/

http://www.kb.cert.org/vuls/id/310295

http://www.microsoft.com/isaserver/downloads/sp1.asp

http://www.microsoft.com/isaserver/evaluation/productguide.asp

http://www.microsoft.com/ntserver/ProductInfo/faqs/PPTPfaq.asp

http://www.microsoft.com/windows2000/techinfo/reskit/en-us/default.asp?url=/WINDOWS2000/techinfo/reskit/en-us/cnet/cnfc_por_simw.asp

http://www.microsoft.com/windows2000/techinfo/reskit/en-us/default.asp?url=/WINDOWS2000/techinfo/reskit/en-us/intwork/inbe_vpn_HIDV.asp

http://www.microsoft.com/windows2000/techinfo/reskit/en-us/default.asp?url=/WINDOWS2000/techinfo/reskit/en-us/intwork/inbe_vpn_obwd.asp

http://www.microsoft.com/windows2000/techinfo/reskit/en-us/default.asp?url=/WINDOWS2000/techinfo/reskit/en-us/deploy/dgcf_inc_bhah.asp

http://www.microsoft.com/WINDOWS2000/techinfo/reskit/samplechapters/inbe/inbe_vpn_hueq.asp

http://www.microsoft.com/WINDOWS2000/techinfo/reskit/samplechapters/inbe/inbe_vpn_hueq.asp

http://www.microsoft.com/windowsxp/home/using/productdoc/en/default.asp?url=/WINDOWSXP/home/using/productdoc/en/auth_eap.asp

http://www.mikersoft.com/ant/ant_help_shares.html

http://www.nwfusion.com/news/2001/0817msisa.html

http://www.nwinternet.com/~pchelp/bo/bo.html

http://www.pentics.net/denial-of-service/white-papers/smurf.cgi

http://www.powertech.no/smurf/

http://www.rawlogic.com/products.html

http://www.sans.org/y2k/practical/Vince_Berk_GCFW.zip

http://www.securityspace.com/smysecure/daudit_faq.html

http://www.sub-seven.com/freeware.shtml

http://www.symantec.com/avcenter/venc/data/smurf.dos.attack.html

http://www.sys-exp.com/win2k/hardenW2K12.pdf

http://www.sys-exp.com/win2k/HardenWin2K.html

http://www.webopedia.com/TERM/c/clustering.html

http://www.webopedia.com/TERM/D/DDR.html

http://www.webopedia.com/TERM/N/NTFS.html

http://www.webopedia.com/TERM/P/proxy_server.html

http://www.webopedia.com/TERM/s/spoof.html

http://www.webopedia.com/TERM/T/Trojan_horse.html

http://www.webopedia.com/TERM/T/TTL.html

http://www.webopedia.com/TERM/V/VPN.html

http://www.wemanageservers.com/managed_security/security_audit/security_audit.html

http://security.uchicago.edu/seminars/DDoS/tfn.shtml

http://staff.washington.edu/dittrich/misc/tfn.analysis

http://www.cisco.com/warp/public/707/newsflash.html

http://rexgrep.tripod.com/rexfbdmain.htm

http://www.bocklabs.wisc.edu/~janda/macro_faq.html#WM01

http://www.techarts.com/products/escan/default.asp

http://www.techarts.com/products/mailscan/default.asp

http://www.webopedia.com/TERM/C/Content_Vectoring_Protocol.html

http://www.eliashim.com/esafe/default.asp?cf=tl